

ASDM, livre 1 : Guide de configuration ASDM pour l'exploitation générale de la gamme Cisco ASA

Dernière modification : 2026-11-03

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. Tous droits réservés.

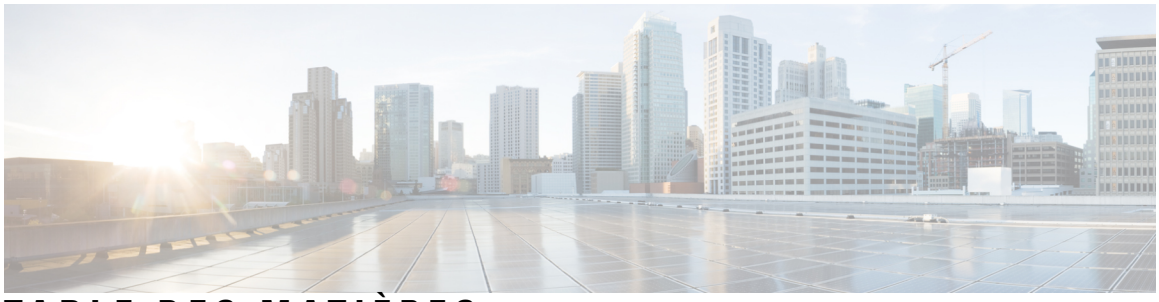


TABLE DES MATIÈRES

PRÉFACE

À propos de ce guide liii

Objectifs du document liii

Documentation associée liii

Conventions de document liii

Communications, services et renseignements supplémentaires lv

PARTIE I

Mise en route de l'ASA 57

CHAPITRE 1

Introduction à Secure Firewall ASA 1

Exigences ASDM 1

Exigences ASDM Java 1

Notes de compatibilité ASDM 2

Compatibilité matérielle et logicielle 6

Compatibilité VPN 6

Nouvelles fonctionnalités 6

Nouvelles fonctionnalités dans ASDM 7.19(1.95) 7

Nouvelles fonctionnalités dans ASDM 7.19(1.90) 7

Nouvelles fonctionnalités dans l'ASA 9.19(1)/ASDM 7.19(1) 7

Présentation fonctionnelle du pare-feu 10

Présentation de la politique de sécurité 11

Autorisation ou refus de trafic avec critères d'accès 11

Application de la NAT 11

Protection contre les fragments IP 11

Application du filtrage HTTP, HTTPS ou FTP 11

Application de l'inspection des applications 11

Application des politiques de QoS 11

Application des limites de connexion et de la normalisation TCP 12
Activation de la détection des menaces 12
Présentation du mode pare-feu 12
Présentation de l'inspection dynamique 13
Présentation fonctionnelle VPN 14
Présentation du contexte de sécurité 14
Présentation de la mise en grappe d'ASA 15
Services spéciaux, obsolètes et existants 15

CHAPITRE 2 **Pour commencer 17**
Accéder à la console de l'interface de commande en ligne 17
Accéder à la console de l'ISA 3000 17
Accéder à la console du mode plateforme de Firepower 2100 18
Accès à la console Firepower 1000, 2100 en mode appareil et Secure Firewall 3100 21
Accéder à la console ASA sur le Châssis Firepower 4100/9300 22
Activer le mode FIPS 24
Configurer l'accès ASDM 25
Utiliser la configuration d'usine par défaut pour l'accès ASDM 25
Personnaliser l'accès ASDM 26
Démarrer ASDM 28
Personnaliser le fonctionnement ASDM 30
Installer un certificat d'identité pour ASDM 30
Augmenter la mémoire de configuration de l'ASDM 30
Augmenter la mémoire de configuration de l'ASDM sous Windows 30
Augmenter la mémoire de configuration de l'ASDM sous Mac OS 31
Configurations d'usine par défaut 32
Rétablir les valeurs par défaut de la configuration 33
Restaurer la configuration du déploiement de l'ASA virtuel 36
Configuration par défaut de Firepower 1010 36
Configuration par défaut de Firepower 1100 38
Configuration par défaut du mode plateforme de Firepower 2100 39
Configuration par défaut du mode appareil de Firepower 2100 41
Configuration par défaut de Secure Firewall 3100 42
Configuration par défaut de Châssis Firepower 4100/9300 43

Configuration par défaut d'ISA 3000 44
Configuration du déploiement ASA virtuel 45
Régler le Firepower 2100 en mode appareil ou plateforme 47
Commencer avec la configuration 49
Utiliser l'outil d'interface de ligne de commande dans ASDM 50
Utiliser l'outil d'interface de ligne de commande 50
Afficher les commandes ignorées par ASDM sur l'appareil 51
Appliquer les modifications de configuration aux connexions 51

CHAPITRE 3 **Interface graphique utilisateur ASDM 53**
À propos de l'interface utilisateur d'ASDM 53
Navigation dans l'interface utilisateur d'ASDM 56
Menus 57
Menu Fichier 57
Menu d'affichage 58
Menu Outils 60
Menu Wizards (Assistants) 61
Menu de la fenêtre 62
Menu d'aide 62
Barre d'outils 63
Assistant ASDM 64
Barre d'état 65
Connexion au périphérique 65
Liste des périphériques 65
Boutons communs 66
Raccourcis clavier 67
Trouver une fonction dans les volets ASDM 69
Trouver une fonction dans les listes de règles 69
Activation de la prise en charge étendue des lecteurs d'écran 70
Dossier organisationnel 71
Volet d'accueil (mode unique et contexte) 71
Onglet Device Dashboard (Tableau de bord des périphériques) 71
Volet Device Information (Informations sur le périphérique) 72
Volet d'état de l'interface 74

Volet des sessions VPN 74
Volet d’état de basculement 74
Volet d’état des ressources système 74
Panneau de l’état du trafic 74
Derniers messages Syslog d’ASDM 75
Onglet Tableau de bord du pare-feu 76
Volet de présentation du trafic 77
Volet des 10 principales règles d’accès 77
Volet d’état de l’utilisation maximale 77
Volet des dix principaux serveurs protégés sous attaque SYN 78
Volet des 200 principaux hôtes 78
Volet de résultats du filtre de trafic du réseau de zombies 78
Onglet Tableau de bord de la grappe 79
Onglet Cluster Firewall Dashboard (Tableau de bord du pare-feu de grappe) 80
Onglet Content Security (Sécurité du contenu) 81
Onglet Intrusion Prevention (Prévention contre les intrusions) 82
Onglet ASA CX Status (État de l’ASA CX) 84
Onglets d’état ASA FirePower 84
Volet d’accueil (système) 85
Définir les préférences ASDM 86
Rechercher avec l’assistant ASDM 89
Activation des mesures d’historique 89
Commandes non prises en charge 90
Commandes ignorées et d’affichage uniquement 90
Effets des commandes non prises en charge 91
Masques de sous-réseau discontinus non pris en charge 91
Commandes utilisateur interactives non prises en charge par l’outil CLI ASDM 91

CHAPITRE 4 **Licences : licence à clé d’autorisation de produit pour l’ISA 3000 93**
À propos des licences PAK 93
Licence préinstallée 93
Licence permanente 93
Licences à durée limitée 94
Lignes directrices relatives à l’activation de la licence à durée limitée 94

Fonctionnement de la minuterie des licences à durée limitée 94
Association des licences permanentes et à durée limitée 94
Empilage des licences à durée limitée 95
Échéance de la licence à durée limitée 96
Remarques relatives à la licence 96
LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement 96
Autre licence VPN 96
Nombre total de sessions VPN combinées, tous types 97
Équilibrage de la charge VPN 97
Licences VPN existantes 97
Licence de chiffrement 97
Nombre total de sessions de mandataire TLS 97
Nombre maximum de VLAN 98
Licences partagées Secure Client (services client sécurisés) Premium (AnyConnect 3 et versions antérieures) 98
Licences de basculement 99
Exigences et exceptions en matière de licence de basculement 99
Association des licences de basculement 99
Perte de communication entre les unités de basculement 100
Mise à niveau des paires de basculement 100
Aucun modèle de chiffrement des données utiles 100
FAQ sur les licences 100
Lignes directrices relatives aux licences PAK 101
Configurer les licences PAK 103
Commander des licences PAK et obtenir une clé d'activation 103
Obtenir une licence de cryptage renforcé 104
Activer ou désactiver les clés 107
Configurer une licence partagée (Secure Client (services client sécurisés) 3 et versions antérieures) 108
À propos des licences partagées 108
À propos du serveur de licences partagées et des participants 108
Problèmes de communication entre le participant et le serveur 109
À propos du serveur de sauvegarde de licences partagées 110
Licences de basculement et partagées 110
Nombre maximum de participants 112

Configurer le serveur de licences partagées 112
Configurer le participant à la licence partagée et le serveur de sauvegarde facultatif 113
Licences de fonctionnalités prises en charge par modèle 113
Licences par modèle 114
Fonctionnalités de la licence ISA 3000 114
Supervision des licences PAK 115
Affichage de votre licence actuelle 115
Supervision de la licence partagée 116
Historique des licences PAK 116

CHAPITRE 5 **Licences : gestion des licences logicielles Smart 125**
À propos des licences logicielles Smart 125
Licences logicielles Smart pour l'ASA sur le Châssis Firepower 4100/9300 126
Gestionnaire de logiciels et comptes Smart 126
Gestion hors ligne 127
Réservation de licence permanente 127
Smart Software Manager sur place 131
Licences et appareils gérés par compte virtuel 131
Licence d'évaluation. 131
À propos des licences par type 132
LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement 133
Autres homologues VPN 133
Total des homologues VPN combinés, tous types 133
Licence de chiffrement 133
Licence d'opérateur 136
Nombre total de sessions de mandataire TLS 136
Nombre maximum de VLAN 137
Licence de filtre de trafic de réseau de zombies 137
Licences de basculement ou de grappe ASA 137
Licences de basculement pour l'ASAv 137
Licences de basculement pour Firepower 1010 137
Licences de basculement pour Firepower 1100 138
Licences de basculement pour Firepower 2100 140
Licences de basculement pour Cisco Secure Firewall 3100 141

Licences de basculement pour le Firepower 4100/9300 143
Licences de grappe ASA pour Cisco Secure Firewall 3100 144
Licences de grappe ASA pour l'ASAv 145
Licences de grappe ASA pour l'Firepower 4100/9300 146
Conditions préalables à la gestion de licences logicielles Smart 147
Conditions préalables de Smart Software Manager standard et sur site 147
Conditions préalables à la réservation de licence permanente 148
Gestion des licences logicielles Smart 148
Paramètres par défaut des licences logicielles Smart 149
ASA virtuel : configurer les licences logicielles Smart 149
ASA virtuel : configurer les licences logicielles Smart standard 149
ASA virtuel : configurer les licences Smart Software Manager sur site 153
ASA virtuel: configurer les licences logicielles Smart Utility (MSLA) 155
ASA virtuel: configurer la réservation de licence permanente 159
Installer la licence permanente ASA virtuel 159
(Facultatif) Retourner la licence permanente ASA virtuel 161
(Facultatif) Annuler l'enregistrement de l'ASA virtuel (standard et sur site) 162
(Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASA virtuel (standard et sur site) 163
Firepower 4100/9300 : configuration de la licence logicielle Smart 163
Autres modèles : configurer les licences logicielles Smart 164
Autres modèles : configurer les licences logicielles Smart standard 165
Autres modèles : configuration des licences Smart Software Manager sur site 170
Autres modèles : configuration de la réservation de licence permanente 173
Installation de la licence permanente 1000/2100/3100 173
(Facultatif) Autres modèles : retour de la licence permanente 176
(Autres modèles) Dérégistrer l'ASA (standard et sur site) 177
(Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASAv (standard et sur site) 178
Licences par modèle 178
ASA virtuel 178
Firepower 1010 183
Gamme Firepower 1100 184
Firepower Série 2100 186
Gamme Secure Firewall 3100 187

Firepower 4100 188
Firepower 9300 190
Supervision des licences logicielles Smart 190
Affichage de votre licence actuelle 191
Affichage de l'état de la licence Smart 191
Affichage de l'UDI 191
Communication avec Smart Software Manager 191
Enregistrement de l'appareil et jetons 191
Communication périodique avec le Smart Software Manager 192
État de non-conformité 192
Infrastructure Smart Call Home 193
Gestion des certificats de licence Smart 193
Historique des licences logicielles Smart 194

CHAPITRE 6 **Périphériques logiques pour le Firepower 4100/9300** 199
À propos des interfaces 199
Interface de gestion de châssis 199
Types d'interface 200
Interfaces FXOS par rapport aux interfaces d'application 201
À propos des périphériques logiques 202
Périphériques logiques autonomes et en grappe 202
Exigences et conditions préalables pour les combinaisons matérielles et logicielles 203
Lignes directrices et limites relatives aux périphériques logiques 204
Lignes directrices et limites des interfaces 204
Lignes directrices et limites générales 204
Exigences et prérequis pour la haute accessibilité 205
Interfaces de configuration 205
Activer ou désactiver une interface 205
Configurer une interface physique 206
Ajouter un canal EtherChannel (canal de port) 207
Configurer les périphériques logiques 209
Ajouter un ASA autonome 210
Ajouter une paire à haute disponibilité 213
Modifier une interface sur un périphérique logique ASA 213

Se connecter à la console de l'application 214
Historique des périphériques logiques 216

CHAPITRE 7 **Mode pare-feu transparent ou routé 219**
Mode pare-feu 219
Mode de pare-feu routé 219
Mode de pare-feu transparent 220
Utilisation d'un réseau de pare-feu transparent 220
Interface Management (gestion) 220
Passage de trafic pour les fonctionnalités en mode routé 221
Groupes de ponts 221
Interfaces virtuelles de pont 221
Groupes de ponts en mode pare-feu transparent 222
Groupes de ponts en mode pare-feu routé 222
Transmission du trafic non autorisée en mode routé 223
Autorisation du trafic de couche 3 224
Adresses MAC autorisées 224
BPDU Handling (gestion des paquets BPDU) 224
Recherches d'adresse MAC ou de route 225
Fonctionnalités non prises en charge pour les groupes de ponts en mode transparent 227
Fonctionnalités non prises en charge pour les groupes de ponts en mode routé 228
Paramètres de défaut 229
Lignes directrices sur le mode pare-feu 229
Définir le mode du pare-feu (mode unique) 231
Exemples de mode de pare-feu 232
Progression des données dans l'ASA en mode de pare-feu routé 232
Un utilisateur interne visite un serveur web 232
Un utilisateur externe visite un serveur web sur la DMZ 234
Un utilisateur interne visite un serveur web sur la DMZ 235
Un utilisateur externe tente d'accéder à un hôte interne 235
Un utilisateur DMZ tente d'accéder à un hôte interne 236
Progression des données dans le pare-feu transparent 237
Un utilisateur interne visite un serveur web 238
Un utilisateur interne visite un serveur web à l'aide de la NAT 239

Un utilisateur externe visite un serveur web sur le réseau interne 241
Un utilisateur externe tente d'accéder à un hôte interne 242
Historique du mode de pare-feu 243

CHAPITRE 8 Assistant de démarrage 247
Accès à l'assistant de démarrage 247
Lignes directrices relatives à l'assistant de démarrage 247
Écrans de l'assistant de démarrage 247
Point de départ ou accueil 247
Configuration de base 248
Écrans d'interface 248
Configuration de l'interface externe (mode routé) 248
Configuration de l'interface externe – PPPoE (mode routé, mode unique) 248
Configuration de l'adresse IP de gestion (mode transparent) 248
Configuration des interfaces 248
Routes statiques 248
Serveur DHCP 248
Traduction d'adresses réseau (NAT/PAT) 249
Accès administratif 249
Configuration de base de l'IPS 249
Configuration de base ASA CX (ASA 5585-X) 249
Configuration de base ASA FirePOWER 249
Configuration du fuseau horaire et de l'horloge 249
Serveur de mise à jour automatique (mode unique) 249
Résumé de l'assistant de démarrage 250
Historique de l'assistant de démarrage 250

PARTIE II Fonctionnalités de haute disponibilité et d'évolutivité 253

CHAPITRE 9 Mode contexte multiple 255
À propos des contextes de sécurité 255
Utilisations courantes des contextes de sécurité 255
Fichiers de configuration de contexte 256
Configurations de contexte 256

Configuration système 256
Configuration du contexte d'administration 256
Classement des paquets par l'ASA 256
Critères de classificateurs valides 256
Exemples de classement 257
Contextes de sécurité en cascade 260
Accès de gestion aux contextes de sécurité 261
Accès à l'administrateur système 261
Accès à l'administrateur de contexte 261
Utilisation de l'interface de gestion 262
À propos de la gestion des ressources 262
Classes des ressources 262
Limites des ressources 262
Classe par défaut 263
Utiliser des ressources surexploitées 264
Utiliser des ressources illimitées 264
À propos des adresses MAC 265
Adresses MAC en mode de contexte multiple 265
Adresses MAC automatiques 265
Prise en charge du VPN 266
Licences pour le mode de contexte multiple 267
Conditions préalables pour le mode de contexte multiple 268
Lignes directrices pour le mode de contexte multiple 268
Paramètres par défaut du mode de contexte multiple 269
Configurer plusieurs contextes 269
Activer ou désactiver le mode de contexte multiple 270
Activer le mode de contexte multiple 270
Rétablir le mode de contexte unique 272
Configurer une classe pour la gestion des ressources 272
Configurer un contexte de sécurité 276
Attribuer automatiquement des adresses MAC aux interfaces de contexte 279
Changer entre les contextes et l'espace d'exécution du système 280
Gérer les contextes de sécurité 280
Supprimer un contexte de sécurité 280

Modifier le contexte d'administration 281
Modifier l'URL du contexte de sécurité 282
Recharger un contexte de sécurité 283
Recharger en effaçant la configuration 283
Recharger en supprimant et en rajoutant le contexte 283
Supervision des contextes de sécurité 284
Superviser l'utilisation des ressources de contexte 284
Afficher les adresses MAC attribuées 286
Afficher les adresses MAC dans la configuration système 286
Afficher les adresses MAC dans un contexte 286
Historique du mode de contexte multiple 287

CHAPITRE 10 **Basculement pour la haute disponibilité 293**
À propos du basculement 293
Modes de basculement 293
Configuration système requise Basculement 294
Configuration matérielle requise 294
Exigences relatives au logiciel 295
Exigences de licence 295
Liaisons de basculement et de basculement avec état 295
Liaison de basculement 296
Liaisons de basculement dynamique 298
Éviter le basculement interrompu et les liaisons de données 299
Les adresses MAC et les adresses IP en Basculement 300
Basculement avec et sans état 302
Basculement sans état 303
Basculement avec état 303
Exigences en matière de groupes de ponts pour le basculement 305
Exigences en matière de groupes de ponts pour les appareils, ASAv 305
Supervision de l'intégrité du basculement 306
Surveillance de l'intégrité de l'unité 306
Supervision des interfaces 307
et seuils de délai de détection 309
Synchronisation de la configuration 310

Réplication de la configuration en cours d'exécution 310
Réplication du fichier 311
Réplication de la commande 312
Optimisation de la synchronisation de la configuration 312
Basculement actif/de secours 314
Rôles principal/secondaire et état actif/de secours 314
Détermination de l'unité active au démarrage 315
Événements de basculement 315
À propos du basculement actif/actif 316
Présentation du basculement actif/actif 316
Rôles principal/secondaire et état actif/de secours pour un groupe de basculement 317
Détermination de l'unité active pour les groupes de basculement au démarrage 317
Événements de basculement 317
Licences pour le basculement 319
Lignes directrices pour Basculement 319
Paramètres par défaut pour le basculement 323
Configurer le basculement actif/de secours 323
Configurer le basculement actif/actif 325
Configurer les paramètres de basculement facultatifs 326
Configurer les critères de basculement et les autres paramètres 326
Configurer la supervision de l'interface et les adresses en veille 330
Configurer la prise en charge des paquets routés asymétriques (mode actif/actif) 331
Gérer Basculement 333
Modifier la configuration du basculement 333
Forcer le basculement 336
Désactiver le basculement 337
Restaurer une unité défaillante 337
Resynchroniser la configuration 338
Surveillance de Basculement 338
Messages de basculement 338
Messages de journal système de basculement 339
Messages de débogage de basculement 339
Interruptions de basculement SNMP 339
Supervision de l'état du basculement 339

Système 339
Groupe de basculement 1 et groupe de basculement 2 340
Historique de basculement 341

CHAPITRE 11 **Basculement pour la haute disponibilité dans le nuage public 345**
À propos du basculement dans le nuage public 345
À propos du basculement actif/de secours 346
Rôles principal/secondaire et état actif/de secours 346
Connexion de basculement 346
Messages de sondage et Hello 347
Détermination de l'unité active au démarrage 347
Événements de basculement 347
Lignes directrices et limites relatives à la licence 349
Licences pour le basculement dans le nuage public 350
Valeurs par défaut pour le basculement dans le nuage public 350
À propos de l'ASA virtuel à haute disponibilité dans Microsoft Azure 351
À propos du principal de service Azure 353
Exigences de configuration pour ASA virtuel haute disponibilité dans Azure 354
Configurer le basculement actif/de secours 354
Configurer les paramètres de basculement facultatifs 357
Configurer les tableaux de routage Azure 357
Gérer le basculement dans le nuage public 358
Forcer le basculement 358
Mettre à jour les routes 359
Valider l'authentification Azure 359
Superviser le basculement dans le nuage public 360
État de basculement 360
Messages de basculement 360
Historique de basculement dans le nuage public 361

CHAPITRE 12 **Grappe ASA pour le Secure Firewall 3100 363**
À propos de la mise en grappe d'ASA 363
Intégration d'une grappe à votre réseau 363
Membres de la grappe 364

Configuration du démarrage 364
Rôles des nœuds de contrôle et de données 364
Interfaces de grappe 364
Liaisons de commande de grappe 365
Réplication de la configuration 365
Gestion de la grappe ASA 365
Réseau de gestion 365
Interface de gestion 365
Gestion de l'unité de contrôle vs Gestion de l'unité de données 366
duplication de clé de chiffrement 366
Incompatibilité d'adresse IP du certificat de connexion ASDM 366
Mise en grappe inter-sites 367
Licences pour la mise en grappe d'ASA 367
Exigences et conditions préalables à la mise en grappe ASA 369
Lignes directrices de la mise en grappe 370
Configurer la mise en grappe ASA 377
Sauvegarder vos configurations (conseillé) 377
Câbler les unités et configurer les interfaces 377
Interfaces de grappe 377
Câbler les unités de grappe et configurer les équipements en amont et en aval 383
Configurer le mode d'interface de grappe sur l'unité de contrôle 384
(Recommandé; requis en mode de contexte multiple) Configurer les interfaces sur le nœud de contrôle 387
Créer ou joindre une grappe à l'aide de l'assistant de haute disponibilité 392
Personnaliser l'opération de mise en grappe 396
Configurer les paramètres de grappe ASA de base 396
Configurer les paramètres de surveillance de l'intégrité de l'interface et de jonction automatique 402
Configurer le délai de réplication TCP de la grappe 404
Configurer les fonctionnalités inter-sites 404
Gérer les nœuds de la grappe 408
Ajouter un nouveau nœud de données à partir du nœud de contrôle 408
Devenir un nœud inactif 409
Désactiver un nœud de données du nœud de contrôle 410
Rejoindre la grappe 411

Quitter la grappe 412
Modifier le nœud de contrôle 413
Exécuter une commande à l'échelle de la grappe 414
Supervision de la grappe ASA 415
Supervision de l'état de la grappe 415
Capture des paquets à l'échelle de la grappe 415
Supervision des ressources de la grappe 416
Supervision du trafic de la grappe 416
Supervision de la liaison de commande de grappe 416
Supervision du routage de la grappe 416
Configuration de la journalisation pour la mise en grappe 417
Exemples de mise en grappe ASA 417
Exemple de configuration ASA et du commutateur 417
Configuration ASA 417
Configuration du commutateur Cisco IOS 419
Pare-feu sur une seule interface 419
Séparation du trafic 422
Configuration OTV pour la mise en grappe inter-sites en mode routé 424
Exemples de mise en grappe inter-sites 427
Exemple de mode de routage EtherChannel étendu avec des adresses MAC et IP propres au site 427
Exemple intersites nord-sud de mode transparent de l'EtherChannel étendu 428
Exemple inter-sites est-ouest en mode transparent de l'EtherChannel étendu 430
Référence pour la mise en grappe 432
Fonctionnalités et mise en grappe de l'ASA 432
Fonctionnalités non prises en charge par la mise en grappe 432
Fonctionnalités centralisées pour la mise en grappe 433
Fonctionnalités appliquées aux nœuds individuels 433
AAA pour l'accès réseau et la mise en grappe 434
Paramètres de connexion et mise en grappe 434
FTP et mise en grappe 434
Inspection ICMP et mise en grappe 435
Routage multidiffusion et mise en grappe 435
NAT et mise en grappe 435
Routage et mise en grappe dynamiques 435

SCTP et mise en grappe 437
Inspection SIP et mise en grappe 437
SNMP et mise en grappe 437
STUN et mise en grappe 437
Syslog, NetFlow et mise en grappe 437
Cisco TrustSec et la mise en grappe 437
VPN et mise en grappe 438
Facteur d'évolutivité de rendement 438
Élection du nœud de contrôle 438
Haute accessibilité au sein des grappes 439
Supervision de l'intégrité du nœud 439
Supervision des interfaces 440
État après l'échec 440
Rejoindre la grappe 440
duplication de l'état de la connexion du chemin de données 441
Gestion des connexions par la grappe 442
Rôles de connexion 442
Nouvelle propriété de connexion 444
Exemple de flux de données pour TCP 444
Exemple de flux de données pour ICMP et UDP 446
Rééquilibrage des nouvelles connexions TCP dans la grappe 448
Historique de la mise en grappe d'ASA pour le Secure Firewall 449

CHAPITRE 13 **Grappe ASA pour le Firepower 4100/9300 451**
À propos de la mise en grappe sur les châssis Firepower 4100/9300 451
Configuration du démarrage 452
Membres de la grappe 452
Liaison de commande de grappe 453
Dimensionnement de la liaison de commande de grappe 453
Redondance de la liaison de commande de la grappe 454
Fiabilité de la liaison de commande de grappe pour la mise en grappe 454
Réseau de liaison de commande de grappe 454
Test de ping de la MTU de la liaison de commande de grappe 455
Interfaces de la grappe 455

Connexion à un système de commutateurs redondants 455
Réplication de la configuration 456
Gestion des grappes Cisco Secure Firewall ASA 456
Réseau de gestion 456
Interface de gestion 456
Gestion de l'unité de contrôle vs Gestion de l'unité de données 456
duplication de clé de chiffrement 457
Incompatibilité d'adresse IP du certificat de connexion ASDM 457
EtherChannels étendus (recommandé) 457
Mise en grappe inter-sites 458
Exigences et conditions préalables à la mise en grappe sur Châssis Firepower 4100/9300 459
Licences pour la mise en grappe sur le Châssis Firepower 4100/9300 461
Lignes directrices et limites de la mise en grappe 462
Configurer la mise en grappe sur le Châssis Firepower 4100/9300 467
FXOS : Ajouter une grappe ASA 468
Créer une grappe ASA 468
Ajouter d'autres membres à la grappe 474
ASA : Modifier le mode de pare-feu et le mode de contexte 476
ASA : Configurer les interfaces de données 476
ASA : Personnaliser la configuration de la grappe 479
Configurer les paramètres de grappe ASA de base 479
Configurer les paramètres de surveillance de l'intégrité de l'interface et de jonction automatique 483
Configurer le délai de réplication TCP de la grappe 484
Configurer les fonctionnalités inter-sites 485
Configurer le VPN de site à site distribué 488
FXOS : supprimer un nœud de la grappe 495
ASA : Gérer les membres de la grappe 496
Devenir un membre inactif 496
Désactiver une unité de données de l'unité de contrôle 497
Rejoindre la grappe 498
Changer l'unité de contrôle 499
Exécuter une commande à l'échelle de la grappe 499
ASA : supervision de la grappe ASA sur le Châssis Firepower 4100/9300 501
Supervision de l'état de la grappe 501

Capture des paquets à l'échelle de la grappe 501
Supervision des ressources de la grappe 501
Supervision du trafic de la grappe 502
Supervision de la liaison de commande de grappe 502
Supervision du routage de la grappe 502
Supervision du VPN S2S distribué 502
Configuration de la journalisation pour la mise en grappe 503
Dépannage du VPN S2S distribué 503
Exemples de mise en grappe d'ASA 504
Pare-feu sur une seule interface 505
Ségrégation du trafic 508
Configuration OTV pour la mise en grappe inter-sites en mode routé 510
Exemples de mise en grappe inter-sites 513
Exemple de mode de routage EtherChannel étendu avec des adresses MAC et IP propres au site 513
Exemple intersites nord-sud de mode transparent de l'EtherChannel étendu 514
Exemple inter-sites est-ouest en mode transparent de l'EtherChannel étendu 516
Référence pour la mise en grappe 518
Fonctionnalités et mise en grappe de l'ASA 518
Fonctionnalités non prises en charge par la mise en grappe 518
Fonctionnalités centralisées pour la mise en grappe 519
Fonctionnalités appliquées aux unités individuelles 520
AAA pour l'accès réseau et la mise en grappe 520
Paramètres de connexion 520
FTP et mise en grappe 520
Inspection ICMP 521
Routage multidiffusion et mise en grappe 521
NAT et mise en grappe 521
Routage et mise en grappe dynamiques 524
SCTP et mise en grappe 525
Inspection SIP et mise en grappe 525
SNMP et mise en grappe 526
STUN et mise en grappe 526
Syslog, NetFlow et la mise en grappe 526
Cisco TrustSec et la mise en grappe 526

VPN et mise en grappe sur le châssis Secure Firewall eXtensible Operating System (FXOS) 526
Facteur d'évolutivité de rendement 527
Choix d'unité de contrôle 527
Haute disponibilité au sein de la grappe 528
Surveillance des applications du châssis 528
Surveillance de l'intégrité de l'unité 528
Surveillance d'interfaces 528
Surveillance de l'application Decorator 529
État après l'échec 529
Rejoindre la grappe 529
Réplication de l'état de la connexion du chemin de données 530
Gestion des connexions par la grappe 530
Rôles de connexion 531
Nouvelle propriété de connexion 533
Exemple de flux de données pour TCP 533
Exemple de flux de données pour ICMP et UDP 535
Rééquilibrage des nouvelles connexions TCP dans la grappe 537
Historique de la mise en grappe d'ASA sur le Firepower 4100/9300 537

CHAPITRE 14 **Grappe ASA pour l'ASA virtuel pour le cloud privé 547**
À propos de la mise en grappe d'ASA virtuel 548
Intégration de la grappe dans votre réseau 548
Nœuds de la grappe 548
Configuration du démarrage 548
Rôles des nœuds de contrôle et de données 548
Interfaces individuelles 549
Routage à base de règles 550
Routage à chemins multiples à coût égal 551
Liaison de commande de grappe 551
Présentation du trafic de liaison de commande de grappe 552
Échec de la liaison de commande de grappe 552
Test de ping de la MTU de la liaison de commande de grappe 552
Réplication de la configuration 553
Gestion des grappes ASA virtuel 553

Réseau de gestion 553
Interface de gestion 553
Gestion de nœud de contrôle vs Gestion de nœud de données 554
duplication de clé de chiffrement 554
Incompatibilité d'adresse IP du certificat de connexion ASDM 554
Mise en grappe inter-sites 555
Licences pour la mise en grappe d'ASA virtuel 555
Exigences et conditions préalables à la mise en grappe d'ASA virtuel 555
Lignes directrices de la mise en grappe d'ASA virtuel 556
Configurer la mise en grappe d'ASA virtuel à l'aide d'une configuration Day0 557
Configurer la mise en grappe ASA virtuel après le déploiement 560
Sauvegarder vos configurations (conseillé) 560
Configurer les paramètres d'interface 561
Configurer le mode d'interface de grappe sur le nœud de contrôle 561
Configurer la liaison de commande de grappe sur le nœud de contrôle 563
Configurer les interfaces individuelles 565
Créer ou joindre une grappe à l'aide de l'assistant de haute disponibilité 568
Personnaliser l'opération de mise en grappe 571
Configurer les paramètres de grappe ASA de base 571
Configurer les paramètres de surveillance de l'intégrité de l'interface et de jonction automatique 575
Configurer le délai de réplication TCP de la grappe 576
Configurer les fonctionnalités inter-sites 577
Configurer la mobilité des flux de grappes 577
Gérer les nœuds de la grappe 580
Ajouter un nouveau nœud de données à partir du nœud de contrôle 581
Devenir un nœud inactif 582
Désactiver un nœud de données à partir du nœud de contrôle 583
Rejoindre la grappe 583
Quitter la grappe 584
Modifier le nœud de contrôle 585
Exécuter une commande à l'échelle de la grappe 585
Supervision de la grappe ASA virtuel 586
Supervision de l'état de la grappe 586
Capture des paquets à l'échelle de la grappe 587

Supervision des ressources de la grappe 587
Supervision du trafic de la grappe 587
Supervision de la liaison de commande de grappe 588
Supervision du routage de la grappe 588
Configuration de la journalisation pour la mise en grappe 588
Exemples de mise en grappe d'ASA virtuel 588
Exemple inter-sites nord-sud de mode routé d'interface individuelle 588
Référence pour la mise en grappe 589
Fonctionnalités et mise en grappe de l'ASA 589
Fonctionnalités non prises en charge par la mise en grappe 590
Fonctionnalités centralisées pour la mise en grappe 590
Fonctionnalités appliquées aux nœuds individuels 591
AAA pour l'accès réseau et la mise en grappe 592
Paramètres de connexion et mise en grappe 592
Routage et mise en grappe dynamiques 592
FTP et mise en grappe 594
Inspection ICMP et mise en grappe 594
Routage multidiffusion et mise en grappe 594
NAT et mise en grappe 594
SCTP et mise en grappe 596
Inspection SIP et mise en grappe 596
SNMP et mise en grappe 596
STUN et mise en grappe 597
Syslog, NetFlow et la mise en grappe 597
Cisco TrustSec et la mise en grappe 597
VPN et mise en grappe 597
Facteur d'évolutivité de rendement 598
Choix du nœud de contrôle 598
Haute disponibilité au sein de la grappe ASA virtuel 599
Supervision de l'intégrité du nœud 599
Surveillance d'interfaces 599
État après l'échec 599
Rejoindre la grappe 600
Réplication de l'état de la connexion du chemin de données 600

Gestion des connexions par la grappe ASA virtuel 601
Rôles de connexion 601
Nouvelle propriété de connexion 603
Exemple de flux de données pour TCP 603
Exemple de flux de données pour ICMP et UDP 605
Rééquilibrage des nouvelles connexions TCP dans la grappe 607
Historique de la mise en grappe d'ASA virtuel 607

PARTIE III **Interfaces** 609

CHAPITRE 15 **Configuration de l'interface de base** 611
À propos de la configuration de l'interface de base 611
Fonctionnalité Auto-MDI/MDIX 611
Interface de gestion 612
Présentation de l'interface de gestion 612
L'interface de logement/port de gestion 612
Utiliser n'importe quelle interface pour le trafic de gestion uniquement 613
Interface de gestion pour le mode transparent 613
Lignes directrices pour la configuration de l'interface de base 614
Paramètres par défaut pour la configuration de l'interface de base 614
Activer l'interface physique et configurer les paramètres Ethernet 615
Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000) 618
Gérer le module réseau pour Cisco Secure Firewall 3100 619
Configurer les ports d'éclatement 619
Ajouter un module de réseau 620
Échange à chaud du module de réseau 621
Remplacer le module de réseau par un module de type différent 622
Retirer le module de réseau 623
Exemples d'interfaces de base 623
Exemple de paramètres d'interface physique 623
Exemple de mode de contexte multiple 624
Historique de la configuration de l'interface de base 624

CHAPITRE 16 **Configuration de base de l'interface pour les ports de commutation du Firepower 1010** 629

À propos des ports de commutation 629
Comprendre les ports et les interfaces de commutation 629
Fonctionnalité Auto-MDI/MDIX 630
Préalables pour les ports de commutation 630
Lignes directrices relatives aux ports de commutation 631
Configuration des ports de commutation et l'alimentation par Ethernet (PoE) 632
Configurer une interface VLAN 632
Configuration des ports de commutation comme ports d'accès 633
Configuration des ports de commutation comme ports de ligne principale 634
Configurer Power Over Ethernet (alimentation électrique par câble Ethernet) 636
Supervision des ports de commutation 637
Historique des ports de commutation 638

CHAPITRE 17 **Interfaces EtherChannel** 639
À propos des EtherChannels 639
About EtherChannels 639
Interfaces des groupes de canaux 640
Connexion à un EtherChannel sur un autre périphérique 640
Protocole LACP (Link Aggregation Control Protocol) 641
Équilibrage de la charge 642
Adresse MAC de l'EtherChannel 642
Directives pour les EtherChannels 643
Paramètres par défaut pour les interfaces EtherChannels 645
Configurer un EtherChannel 646
Ajouter des interfaces à l'EthernetChannel 646
Personnaliser l'EtherChannel 648
Exemples d'EtherChannels 650
Historique des EtherChannels 650

CHAPITRE 18 **Interfaces de boucle avec retour** 653
À propos des interfaces de boucle avec retour 653
Directives pour les interfaces de boucle avec retour 654
Configurer une interface de boucle avec retour 654
Limite de débit du trafic vers l'interface de boucle avec retour 655

Historique des interfaces de boucle avec retour 659

CHAPITRE 19 **Sous-interfaces VLAN 661**

À propos des sous-interfaces VLAN 661

Licences pour les sous-interfaces VLAN 661

Lignes directrices et limites pour les sous-interfaces VLAN 662

Paramètres par défaut pour les sous-interfaces VLAN 663

Configurer les sous-interfaces VLAN et la jonction 802.1Q 663

Exemples de sous-interfaces VLAN 665

Historique des sous-interfaces VLAN 666

CHAPITRE 20 **Interfaces VXLAN 669**

À propos des interfaces VXLAN 669

Encapsulation 669

Point terminal du tunnel VXLAN 670

Interface de la source VTEP 670

Interface VNIs 671

Traitement de paquet VXLAN 671

Pair VTEP 672

Scénarios VXLAN 673

Présentation du pont ou de la passerelle VXLAN 673

Pont VXLAN 673

Passerelle VXLAN (mode routé) 674

Routeur entre domaines VXLAN 675

Équilibreur de charge de passerelle AWS et serveur mandataire à un seul volet de Geneve 677

Équilibreur de charge de passerelle Azure et serveur mandataire jumelé 678

Exigences et conditions préalables pour les interfaces VXLAN 679

Lignes directrices pour les interfaces VXLAN 680

Paramètres par défaut des interfaces VXLAN 681

Configurer les interfaces VXLAN 681

Configurer l'interface source VTEP 681

Configurer l'interface VNI 682

Configurer les interfaces Geneve 683

Configurer l'interface source VTEP pour Geneve 684

Configurer l'interface VNI pour Geneve 685
Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle 685
Exemples d'interfaces VXLAN 686
Exemple de passerelle VXLAN transparente 687
Exemple de routage VXLAN 689
Historique des interfaces VXLAN 690

CHAPITRE 21 **Interfaces en mode routage et en mode transparent 693**
À propos des interfaces en mode routage et en mode transparent 693
Niveaux de sécurité 694
Double pile IP (IPv4 et IPv6) 694
Masque de sous-réseau 31 bits 694
Sous-réseau 31 bits et mise en grappe 695
Sous-réseau 31 bits et basculement 695
Gestion et sous-réseau 31 bits 695
Fonctionnalités 31 bits non prises en charge 695
Directives et limites pour les interfaces en mode routé et en mode transparent 695
Configurer les interfaces en mode routé 698
Configurer les paramètres généraux de l'interface en mode routé 698
Configurer le protocole PPPoE 701
Configurer les interfaces de groupe de ponts 702
Configurer la BVI (Bridge Virtual Interface) 702
Configurer les paramètres généraux de l'interface de membre du groupe de ponts 704
Configurer une interface de gestion pour le mode transparent 705
Configuration de l'adressage IPv6 707
À propos d'IPv6 707
Adresse IPv6 708
ID d'interface EUI-64 modifiée 708
Configurer le client de délégation de préfixe IPv6 708
À propos de la délégation de préfixe IPv6 708
Activer le client de délégation de préfixe IPv6 711
Configuration d'une adresse globale IPv6 712
(Facultatif) Configurer automatiquement les adresses Link-Local 715
(Facultatif) Configurer manuellement les adresses Link-Local 716

Configurer la découverte des voisins IPv6 716
Afficher et effacer les voisins détectés dynamiquement 720
Supervision des interfaces en mode routé et en mode transparent 720
Statistiques et informations sur l'interface 721
Renseignements sur DHCP 721
Suivi du routage statique 722
PPPoE 722
ACL dynamiques 722
Exemples d'interfaces en mode routé et en mode transparent 723
Exemple de mode transparent avec 2 groupes de ponts 723
Exemple de segment LAN commuté avec 2 groupes de ponts 723
Historique des interfaces en mode routé et en mode transparent 726

CHAPITRE 22 **Configuration avancée de l'interface** 731
À propos des configurations avancées de l'interface 731
À propos des adresses MAC 731
Adresses MAC par défaut 731
Adresses MAC automatiques 732
À propos de la MTU 733
Chemin de découverte de MTU 733
MTU par défaut 733
MTU et fragmentation. 733
MTU et trames grand format 734
À propos de TCP MSS 734
TCP MSS par défaut 734
Paramètre MSS TCP maximal suggéré 735
Communication inter-interface 735
Communication intra-interface (mode de pare-feu routé) 735
Attribuer automatiquement des adresses MAC 736
Configurer l'adresse MAC manuelle, la MTU et le TCP MSS 737
Autoriser la communication de niveau de sécurité identique 738
Supervision de l'ARP et du tableau d'adresses MAC 739
Historique de la configuration avancée de l'interface 739

CHAPITRE 23 **Zones de circulation** 741

À propos des zones de trafic 741

Comportement non zoné 741

Pourquoi utiliser des zones? 741

Routage asymétrique 742

Route perdue 742

Équilibrage de la charge 743

Tables de connexion et de routage par zone 744

Routage ECMP 744

Prise en charge ECMP non zonée 744

Prise en charge ECMP zonée 745

Équilibrage de charges des connexions 745

Basculement vers une route dans une autre zone 745

Politique de sécurité basée sur l'interface 745

Services pris en charge pour les zones de trafic 746

Niveaux de sécurité 746

Interface principale et actuelle pour le flux 746

Rejoindre ou quitter une zone 746

Trafic intra-zone 747

Trafic entrant et sortant 747

Chevauchement d'adresses IP dans une zone 747

Conditions préalables aux zones de trafic 747

Lignes directrices relatives aux zones de trafic 749

Configurer une zone de trafic 750

Supervision des zones de trafic 751

Renseignements sur la zone 751

Connexions de zone 751

Routage de zone 752

Exemple de zones de trafic 753

Historique des zones de trafic 756

PARTIE IV **Paramètres de base** 757

CHAPITRE 24 **Paramètres de base** 759

Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet 759

Régler la date et l'heure 761

Définir la date et l'heure à l'aide du serveur NTP 761

Régler la date et l'heure manuellement 763

Configurer le protocole PTP (Precision Time Protocol) (ISA 3000) 764

Configurer la phrase secrète principale 765

Ajouter ou modifier la phrase secrète principale 766

Désactiver la phrase secrète principale 767

Configurer des serveurs DNS 768

Configurer le contournement matériel et l'alimentation double (Cisco ISA 3000) 771

Modifier les performances et le comportement ASP (Accelerated Security Path) 773

Choisir un modèle de validation transactionnelle de moteur de règles 773

Activer l'équilibrage de charges ASP 775

Supervision du cache DNS 775

Historique des paramètres de base 776

CHAPITRE 25 **Services DHCP et DDNS** 781

À propos des services DHCP et DDNS 781

Serveur DHCPv4 781

Options de DHCP 781

Serveur sans état DHCPv6 782

Agents de relais DHCP 783

Prise en charge du serveur relais DHCP sur VTI 783

Lignes directrices pour les services DHCP et DDNS 784

Configurer le serveur DHCP 786

Activer le serveur DHCPv4 786

Configurer les options DHCPv4 avancées 788

Configurer le serveur sans état DHCPv6 789

Configurer les agents de relais DHCP. 791

Configuration du DNS dynamique 792

Supervision des services DHCP et DDNS 797

Supervision des services DHCP 797

Supervision de l’état DDNS 798
Historique des services DHCP et DDNS 799

CHAPITRE 26 **Certificats numériques 803**
À propos des certificats numériques 803
Cryptographie à clé publique 804
Évolutivité des certificats 805
Paires de clés 805
Point de confiance 806
Inscription de certificat 806
Serveur mandataire pour les demandes SCEP 806
Vérification de la révocation 807
Serveurs CA pris en charge 807
CRL 807
OCSP 809
Certificats et coordonnées de connexion de l’utilisateur 810
Informations d’authentification de l’utilisateur 810
Certificats 810
Lignes directrices pour les certificats numériques 811
Configurer les certificats numériques 814
Configuration des certificats d’identité 814
Ajouter ou importer un certificat d’identité 815
Exporter un certificat d’identité 819
Générer une requête de signature de certificat 820
Installer des certificats d’identité 821
Configuration des autorités de certification 822
Configuration des certificats CA 822
Gérer les certificats de l’utilisateur 827
Configurer les identités de référence 828
Autoriser le chiffrement faible pour les certificats CA 829
Certificat de signataire de code 830
Importer un certificat de signataire de code 830
Exporter un certificat de signataire de code 830
Définir une alerte d’expiration de certificat (pour les certificats d’identité ou CA) 831

Supervision des certificats numériques 832
Historique de gestion des certificats 832

CHAPITRE 27 **Inspection ARP et table des adresses MAC 835**
À propos de l'inspection ARP et de la table des adresses MAC 835
Inspection ARP pour le trafic de groupe de ponts 835
Tableau d'adresses MAC 836
Paramètres d'usine 836
Lignes directrices pour l'inspection ARP et la table d'adresses MAC 837
Configurer l'inspection ARP et les autres paramètres ARP 837
Ajouter une entrée ARP statique et personnaliser d'autres paramètres ARP 837
Activer l'inspection ARP 838
Personnaliser la table des adresses MAC pour les groupes de ponts 839
Ajouter une adresse MAC statique pour les groupes de ponts 839
Configurer l'apprentissage de l'adresse MAC 840
Historique de l'inspection ARP et de la table des adresses MAC 841

PARTIE V **Routage IP 845**

CHAPITRE 28 **Aperçu du routage 847**
Détermination du chemin 847
Types de routage pris en charge 848
Statique ou dynamique 848
Chemin unique ou chemin multiple 848
Non hiérarchique ou hiérarchique 849
État de lien ou vecteur de distance 849
Protocoles Internet pris en charge pour le routage 849
Routage du trafic GRE 850
Table de routage 850
Mode de remplissage de la table de routage 850
Distances administratives pour les routages 851
Sauvegarde des routes dynamiques et statiques flottantes 852
Prise des décisions de transfert 853
Routage dynamique et Basculement 853

Routage et mise en grappe dynamiques 853
Routage dynamique en mode EtherChannel étendu 854
Routage dynamique en mode d'interface individuelle 855
Routage dynamique en mode de contexte multiple 857
Gestion des ressources de routage 857
Table de routage pour le trafic de gestion 858
Identification de l'interface de gestion 859
Routage à chemins multiples à coûts égaux (ECMP) 859
Désactiver les demandes ARP du mandataire 860
Afficher la table de routage 861
Historique de l'aperçu du routage 861

CHAPITRE 29 **Routages statiques et par défaut 863**
À propos des routages statiques et par défaut 863
Routage par défaut 863
Routes statiques 864
Routage vers l'interface null0 pour abandonner le trafic indésirable 864
Priorités de routage 864
Routages en mode de pare-feu transparent et de groupes de ponts 864
Suivi du routage statique 865
Lignes directrices pour les routages statiques et par défaut 865
Configurer les routes par défaut et statiques 866
Configurer une route par défaut 866
Configurer une route statique 867
Configurer le suivi de route statique 868
Supervision d'une route statique ou par défaut 869
Exemples de routes statiques ou par défaut 870
Historique des routes statiques et par défaut 870

CHAPITRE 30 **Routage basé sur une stratégie 873**
À propos du routage basé sur les politiques 873
Pourquoi utiliser le routage basé sur des politiques? 873
Routage à accès égal et sensible à la source 874
Qualité de service 874

Réduction des coûts 875
Partage de la charge 875
Mise en œuvre de PBR 875
Lignes directrices pour le routage basé sur des politiques 875
Configurer le routage basé sur les politiques 877
Historique du routage basé sur des politiques 880

CHAPITRE 31 **Cartes de routage** 883
À propos des cartes de routage 883
Clauses d'autorisation et de refus 884
Valeurs de clause de correspondance et de définition 884
Lignes directrices relatives aux cartes de routage 885
Définir une carte de routage 885
Personnaliser une carte de routage 888
Définir une route pour correspondre à une adresse de destination spécifique 889
Configurer les règles de préfixe 890
Configurer les listes de préfixe 890
Configurer les valeurs de mesure pour une action de routage 891
Exemple de cartes de routage 891
Historique des cartes de routage 892

CHAPITRE 32 **Routage par détection de transfert bidirectionnel (BFD)** 893
À propos du routage BFD 893
Mode asynchrone BFD et fonction d'écho 893
Établissement de la session BFD 894
Négociation de la minuterie BFD 895
Détection de défaillance BFD 895
Scénarios de déploiement BFD 896
Directives pour le routage BFD 896
Configurer BFD 897
Créer le modèle BFD 897
Configurer les interfaces BFD 899
Configurer les cartes BFD 899
Historique du routage BFD 900

CHAPITRE 33 BGP 901

BGP 901

Scénarios d'utilisation de BGP 901

Modifications apportées à la table de routage 902

Sélection du chemin BGP 903

Chemins multiples BGP 904

Lignes directrices BGP 905

Configurer le protocole BGP 906

Activer BGP 906

Définir le meilleur chemin pour un processus de routage BGP 908

Configurer les listes de politiques 909

Configurer les filtres de chemin AS 910

Configurer les règles de communauté 911

Configurer les paramètres de la famille d'adresses IPv4 912

Configurer les paramètres généraux de la famille IPv4 912

Configurer les paramètres d'adresse globale de la famille IPv4 913

Configurer les paramètres de filtrage de la famille IPv4 914

Configurer les paramètres de voisin BGP de la famille IPv4 914

Configurer les paramètres réseau IPv4 918

Configurer les paramètres de redistribution IPv4 919

Configurer les paramètres d'injection de route IPv4 920

Configurer les paramètres de la famille d'adresses IPv6 920

Configurer les paramètres généraux de la famille IPv6 920

Configurer les paramètres d'adresse globale de la famille IPv6 921

Configurer les paramètres de voisin BGP de la famille IPv6 922

Configurer les paramètres réseau IPv6 926

Configurer les paramètres de redistribution IPv6 927

Configurer les paramètres d'injection de route IPv6 927

Supervision BGP 928

Historique de BGP 929

CHAPITRE 34 OSPF 931

Routage OSPF 931

Prise en charge OSPF pour les paquets Fast Hello 933
Conditions préalables à la configuration des paquets Hello rapide d'OSPF 933
À propos de la prise en charge OSPF pour les paquets Hello rapides 933
Différences d'implémentation entre OSPFv2 et OSPFv3 935
Directives pour OSPF 935
Configurer le protocole OSPFv2 938
Configurer une chaîne de clés pour l'authentification 940
Configurer l'ID de routeur OSPFv2 941
Configurer manuellement l'ID de routeur OSPF 941
Comportement de l'ID de routeur lors de la migration 942
Personnaliser le protocole OSPFv2 943
Redistribuer les routes dans OSPFv2 943
Configurer la synthèse des routes lors de la redistribution des routes dans OSPFv2 945
Ajouter une adresse sommaire de route 945
Ajouter ou modifier une adresse sommaire OSPF 946
Configurer la synthèse des routes entre les zones OSPFv2 947
Configurer les paramètres d'interface OSPFv2 947
Configurer les paramètres de zone OSPFv2 951
Configurer les règles de filtre OSPFv2 952
Configurer une NSSA OSPFv2 953
Configurer un ensemble d'adresses IP pour la mise en grappe (OSPFv2 et OSPFv3) 954
Définir les voisins OSPFv2 statiques 956
Configurer les minuteries de calcul de routage 957
Journaliser les voisins en hausse ou en baisse 958
Configurer une chaîne de clés pour l'authentification 958
Configurer le filtrage dans OSPF 960
Configurer un lien virtuel dans OSPF 961
Configurer le protocole OSPFv3 963
Activer OSPFv3 963
Configurer les paramètres d'interface OSPFv3 963
Configurer les paramètres de zone OSPFv3 965
Configurer un voisin de lien virtuel 966
Configurer des interfaces passives OSPFv3 967
Configurer la distance administrative OSPFv3 968

Configurer les minuteries mOSPFv3 969
Définir les voisins OSPFv3 statiques 970
Envoyer les messages du journal système 971
Supprimer les messages du journal système 971
Calculer les coûts récapitulatifs de la route 972
Générer une route externe par défaut dans un domaine de routage OSPFv3 972
Configurer un préfixe de résumé IPv6 973
Redistribuer les routes IPv6 973
Configurer le redémarrage progressif 974
Configuration du redémarrage progressif pour OSPFv2 975
Configurer le redémarrage progressif de Cisco NSF pour OSPFv2 975
Configuration de la minuterie d'attente de redémarrage progressif pour le OSPF 976
Configuration du redémarrage progressif pour OSPFv3 977
Configuration de la minuterie d'attente de redémarrage progressif pour OSPF 977
Supprimer la configuration OSPFv2 978
Supprimer la configuration OSPFv3 978
Exemple de protocole OSPFv2 979
Exemples de protocole OSPFv3 981
Supervision OSPF 982
Historique OSPF 984

CHAPITRE 35 IS-IS 987
À propos d'IS-IS 987
À propos de NET 987
Nom de domaine dynamique IS-IS 988
Types de PDU IS-IS 988
Fonctionnement d'IS-IS sur les circuits multiaccès 990
Choix de l'IS désigné IS-IS 990
Synchronisation LSPDB IS-IS 991
Calcul du chemin le plus court IS-IS 992
Protocole d'arrêt IS-IS 993
Conditions préalables d'IS-IS 993
Lignes directrices relatives à IS-IS 994
Configurer IS-IS 994

Activer le routage IS-IS globalement 994
Activer l'authentification IS-IS 996
Configurer LSP IS-IS 997
Configurer les adresses de résumé IS-IS 999
Configurer NET IS-IS 1000
Configurer les interfaces passives IS-IS 1001
Configurer les interfaces IS-IS 1002
Configurer la famille d'adresses IPv4 IS-IS 1006
Configurer la famille d'adresses IPv6 IS-IS 1010
Supervision IS-IS 1012
Historique d'IS-IS 1013

CHAPITRE 36 EIGRP 1015
À propos d'EIGRP 1015
Lignes directrices relatives à l'EIGRP 1017
Configurer un processus EIGRP 1018
Configurer le protocole EIGRP 1018
Activer EIGRP 1019
Activer le routage Stub EIGRP 1020
Personnaliser l'EIGRP 1021
Définir un réseau pour un processus de routage EIGRP 1021
Configurer les interfaces pour l'EIGRP 1022
Configurer des interfaces passives 1023
Configurer les adresses d'agrégation du résumé sur les interfaces 1024
Modifier la valeur du délai d'interface 1025
Activer l'authentification EIGRP sur une interface 1025
Définir un voisin EIGRP 1027
Redistribuer les routes dans l'EIGRP 1028
Filtrer les réseaux dans l'EIGRP 1030
Personnaliser l'intervalle Hello et le délai de rétention dans l'EIGRP 1031
Désactiver la synthèse automatique des routes 1032
Configurer les informations par défaut dans l'EIGRP 1032
Désactiver l'horizon divisé de l'EIGRP 1034
Redémarrer le processus EIGRP 1034

Supervision de l'EIGRP 1035
Historique d'EIGRP 1036

CHAPITRE 37 **Routage multidiffusion** 1037
Routage multidiffusion 1037
Routage de multidiffusion en mode stub 1038
Routage de multidiffusion PIM 1038
Mode PIM clairsemé 1038
Prise en charge de la multidiffusion PIM propre à la source 1038
Routeur de démarrage PIM (BSR) 1039
Terminologie du routeur de démarrage PIM (BSR) 1040
Concept de groupe de multidiffusion 1040
Adresses de multidiffusion 1041
Mise en grappe 1041
Lignes directrices pour le routage de multidiffusion 1041
Routage multidiffusion activé 1042
Personnaliser le routage multidiffusion 1043
Configurer le routage de multidiffusion Stub et transférer les messages IGMP 1043
Configurer une route de multidiffusion statique 1044
Configurer des fonctionnalités IGMP 1045
Désactiver IGMP sur une interface 1045
Configurer l'appartenance au groupe IGMP 1045
Configurer un groupe IGMP joint statiquement 1046
Contrôler l'accès aux groupes de multidiffusion 1047
Limiter le nombre d'états IGMP sur une interface 1048
Modifier les messages de requête destinés aux groupes de multidiffusion 1048
Modifier la version IGMP 1049
Configurer des fonctionnalités PIM 1050
Activer et désactiver la PIM sur une interface 1050
Configurer une adresse de point de rendez-vous statique 1051
Configurer la priorité des routeurs désignés 1052
Configurer et filtrer les messages de registre PIM 1052
Configurer les intervalles des messages PIM 1053
Configurer une arborescence de routes 1053

Configurer un groupe de multidiffusion 1054
Filtrer les voisins PIM 1055
Configurer un filtre de voisin bidirectionnel PIM 1056
Configurer l'ASA comme candidat BSR 1057
Configurer une limite de multidiffusion 1058
Supervision de PIM 1059
Exemple de routage de multidiffusion 1059
Historique du routage de multidiffusion 1061

PARTIE VI **Serveurs AAA et base de données locale** 1063

CHAPITRE 38 **AAA et base de données locale** 1065
À propos d'AAA et de la base de données locale 1065
Authentification 1065
Autorisation 1066
Comptabilité 1066
Interaction entre authentification, autorisation et traçabilité 1066
Serveurs et groupes de serveurs AAA 1066
À propos de la base de données locale 1068
Prise en charge du basculement 1069
Fonctionnement du basculement avec plusieurs serveurs dans un groupe 1070
Lignes directrices relatives à la base de données locale 1070
Ajouter un compte d'utilisateur à la base de données locale 1070
Tester l'authentification et l'autorisation de la base de données locale 1072
Supervision de la base de données locale 1073
Historique de la base de données locale 1073

CHAPITRE 39 **Serveurs RADIUS pour AAA** 1079
À propos des serveurs RADIUS pour AAA 1079
Méthodes d'authentification prises en charge 1079
Autorisation des utilisateurs pour les connexions VPN 1080
Ensembles d'attributs RADIUS pris en charge 1080
Attributs d'autorisation RADIUS pris en charge 1080
Attributs d'autorisation RADIUS IETF pris en charge 1090

Codes de motif de déconnexion comptable RADIUS 1091
Lignes directrices relatives aux serveurs RADIUS pour AAA 1091
Configurer les serveurs RADIUS pour AAA 1092
Configurer les groupes de serveurs RADIUS 1092
Ajouter un serveur RADIUS à un groupe 1095
Ajouter une invite d'authentification 1097
Tester l'authentification et l'autorisation du serveur RADIUS 1098
Supervision des serveurs RADIUS pour AAA 1099
Historique des serveurs RADIUS pour AAA 1099

CHAPITRE 40 **Serveurs TACACS+ pour AAA** 1101
À propos des serveurs TACACS+ pour AAA 1101
Attributs TACACS+ 1101
Lignes directrices relatives aux serveurs TACACS+ pour AAA 1103
Configurer les serveurs TACACS+ 1103
Configurer les groupes de serveurs TACACS+ 1103
Ajouter un serveur TACACS+ à un groupe 1104
Ajouter une invite d'authentification 1105
Tester l'authentification et l'autorisation des serveurs TACACS+ 1106
Supervision des serveurs TACACS+ pour AAA 1107
Historique des serveurs TACACS+ pour AAA 1108

CHAPITRE 41 **Serveurs LDAP pour AAA** 1109
À propos de LDAP et de l'ASA 1109
Fonctionnement de l'authentification avec LDAP 1109
Hiérarchie LDAP 1110
Rechercher dans la hiérarchie LDAP 1111
Lier à un serveur LDAP 1111
Cartes d'attribut LDAP 1112
Lignes directrices relatives aux serveurs LDAP pour AAA 1113
Configurer les serveurs LDAP pour AAA 1114
Configurer les cartes d'attribut LDAP 1114
Configurer les groupes de serveurs LDAP 1115
Ajouter un serveur LDAP à un groupe de serveurs 1116

Tester l'authentification et l'autorisation du serveur LDAP 1118
Supervision des serveurs LDAP pour AAA 1118
Historique des serveurs LDAP pour AAA 1119

CHAPITRE 42 **Serveurs Kerberos pour AAA** 1121
Lignes directrices relatives aux serveurs Kerberos pour AAA 1121
Configurer les serveurs Kerberos pour AAA 1121
Configurer les groupes de serveurs AAA Kerberos 1121
Ajouter des serveurs Kerberos à un groupe de serveurs Kerberos 1122
Configurer la validation du centre de distribution des clés Kerberos 1123
Superviser les serveurs Kerberos pour AAA 1125
Historique des serveurs Kerberos pour AAA 1125

CHAPITRE 43 **Configurer les serveurs RSA SecurID pour AAA** 1127
À propos des serveurs RSA SecurID 1127
Lignes directrices relatives aux serveurs RSA SecurID pour AAA 1127
Configurer les serveurs RSA SecurID pour AAA 1128
Configurer les groupes de serveurs RSA SecurID pour AAA 1128
Ajouter des serveurs RSA SecurID à un groupe de serveurs SDI 1129
Importer le fichier secret de nœud SDI 1129
Superviser les serveurs RSA SecurID pour AAA 1130
Historique des serveurs RSA SecurID pour AAA 1131

PARTIE VII **Administration système** 1133

CHAPITRE 44 **Accès de gestion** 1135
Configurer l'accès de gestion à distance 1135
Configurer l'accès ASA pour HTTPS, Telnet ou SSH 1135
Configurer l'accès HTTPS pour ASDM, autres clients 1136
Configurer l'accès SSH 1138
Configurer l'accès Telnet 1146
Configurer la redirection HTTP pour l'accès ASDM ou le SSL VPN sans client 1147
Configurer l'accès de gestion sur un tunnel VPN 1148

Configurer l'accès de gestion pour FXOS sur les interfaces de données en mode plateforme Firepower 2100 1149
Modifier le délai d'expiration de la console 1150
Personnaliser une invite de l'interface de ligne de commande 1151
Configurer une bannière de connexion 1152
Définir un quota de sessions de gestion 1154
Configurer AAA pour les administrateurs système 1155
Configurer l'authentification de gestion 1155
À propos de l'authentification de gestion 1155
Configurer l'authentification pour l'interface de ligne de commande ASDM et activer la commande Access 1157
Contrôler l'interface de ligne de commande et l'accès ASDM avec l'autorisation de gestion 1158
Configurer l'autorisation de commande 1160
À propos de l'autorisation de commande 1161
Configurer l'autorisation de commande locale 1162
Configurer les commandes sur le serveur TACACS+ 1163
Configurer l'autorisation de commande TACACS+ 1166
Configurer une politique de mot de passe pour les utilisateurs de base de données locale 1167
Changer votre mot de passe 1169
Activer et afficher l'historique de connexion 1170
Configurer la traçabilité de l'accès de gestion 1170
Récupérer d'un verrouillage 1171
Accès au moniteur 1173
Historique de l'accès de gestion 1173

CHAPITRE 45 **Logiciels et configurations** 1185
Mettre à niveau le logiciel 1185
Charger une image à l'aide de ROMMON (ISA 3000) 1185
Mettre à niveau l'image ROMMON : ISA 3000 1187
Rétrograder votre logiciel 1188
Directives et limites en matière de rétrogradation 1188
Configuration incompatible supprimée après la rétrogradation 1189
Rétrograder l'appareil ASA 1190
Rétrograder le Firepower 2100 en mode plateforme 1191

Rétrograder le Firepower 4100/9300 1191
Rétrograder l'ISA 3000 1192
Gérer les fichiers 1193
Configurer l'accès au fichier 1193
Configurer le mode client FTP 1194
Configurer l'ASA Secure Copy Client 1194
Configurer le chemin du client TFTP pour l'ASA 1195
Ajouter des points de montage 1196
Accéder à l'outil de gestion de fichiers 1198
Transférer des fichiers 1198
Transférer des fichiers entre l'ordinateur local et la mémoire flash 1199
Transférer des fichiers entre le serveur distant et la mémoire flash 1199
Définir l'image ASA, ASDM et la configuration de démarrage 1201
Sauvegarde et restauration de configurations ou d'autres fichiers 1203
Effectuer une sauvegarde ou une restauration complète du système 1203
Avant d'entreprendre la sauvegarde ou la restauration 1203
Sauvegarder le système 1205
Restaurer la sauvegarde 1206
Configurer la sauvegarde et la restauration automatiques (ISA 3000) 1207
Configurer la sauvegarde automatique (ISA 3000) 1207
Configurer la restauration automatique (ISA 3000) 1208
Enregistrer la configuration en cours d'exécution sur un serveur TFTP 1209
Programmer un redémarrage du système 1210
Échange à chaud d'un SSD sur Cisco Secure Firewall 1211
Historique des logiciels et des configurations 1213

CHAPITRE 46 **Automatisation de la réponse pour les événements système** 1217
À propos de l'EEG 1217
Événements pris en charge 1217
Actions sur les applets de gestionnaire d'événements 1218
Destinations de sortie 1218
Lignes directrices pour l'EEG 1219
Configurer l'EEG 1219
Créer un applet de gestionnaire d'événements et configurer les événements 1220

Configurer une action et des destinations pour la sortie d'une action 1221
Exécuter un applet de gestionnaire d'événements 1222
Suivre l'allocation de mémoire et l'utilisation de la mémoire 1222
Supervision de l'EEG 1223
Historique de l'EEG 1223

CHAPITRE 47 **Tests et dépannage 1225**
Récupérer les mots de passe d'activation et Telnet 1225
Récupérer les mots de passe sur l'ISA 3000 1225
Récupérer les mots de passe ou les images sur l'ASA virtuel 1227
Désactiver la récupération du mot de passe pour le matériel ISA 3000 1228
Configurer et exécuter des captures à l'aide de l'Assistant de capture de paquets 1229
Lignes directrices pour la capture des paquets 1232
Sélecteur de trafic d'entrée 1233
Sélecteur de trafic de sortie 1234
Tampons 1234
Résumé 1235
Exécuter des captures 1235
Enregistrer des captures 1235
Utilisation et rapport d'utilisation du processeur (CPU) 1236
Utilisation de vCPU dans l'ASA virtuel 1236
Exemple d'utilisation du processeur 1236
Rapport d'utilisation du CPU VMware 1237
ASA virtuel et graphiques vCenter 1237
Rapports d'utilisation du CPU Amazon CloudWatch 1238
ASA virtuel et graphiques Amazon CloudWatch 1238
Rapport d'utilisation du CPU Azure 1238
Graphiques ASA virtuel et Azure 1239
Rapport d'utilisation du CPU Hyper-V 1239
Graphiques ASA virtuel et Hyper-V 1240
Rapport d'utilisation du CPU OCI 1240
ASA virtuel et graphiques OCI 1241
Tester votre configuration 1241
Tester la connectivité de base : envoi d'un ping à des adresses 1241

Ce que vous pouvez tester en utilisant le ping 1241
Choisir entre le ping ICMP et TCP 1242
Activer le protocole ICMP 1242
Envoyer un message ping à des hôtes 1243
Tester la connectivité ASA de manière systématique 1244
Tracer les routes vers les hôtes 1247
Rendre l'ASA visible sur les routes de trace 1247
Déterminer les routes de paquets 1247
Utiliser l'outil Packet Tracer pour tester la configuration de la politique 1249
Supervision des performances et des ressources du système 1250
Supervision des performances 1250
Supervision des blocs de mémoire 1251
Supervision du CPU 1251
Supervision de la mémoire 1252
Supervision de l'utilisation du CPU par processus 1252
Supervision des connexions 1252
Historique des tests et du dépannage 1253

PARTIE VIII **Surveillance** 1257

CHAPITRE 48 **Journalisation** 1259
À propos de la journalisation 1259
Journalisation dans le mode de contexte multiple 1260
Analyse des messages du journal système 1260
Format des messages du journal système 1261
Niveaux de gravité des messages Syslog 1262
Filtres de messages syslog 1262
Classes de messages syslog et numéros d'ID de messages associés 1263
Trier les messages dans les visionneuses de journaux 1266
Listes de messages personnalisés 1266
Mise en grappe 1266
Lignes directrices relatives à la journalisation 1267
Configurer la journalisation 1269
Activer la journalisation 1269

Configurer une destination de sortie 1270
Envoyer des messages du journal système à un serveur externe de journal système 1270
Envoyer les messages du journal système au tampon du journal interne 1274
Envoyer des messages Syslog à une adresse courriel 1277
Envoyer les messages du journal système au port de console 1279
Envoyer les messages du journal système à une session Telnet ou SSH 1279
Configurer les messages du journal système 1280
Configurer la messagerie du journal système 1280
Modifier les paramètres d'ID du journal système 1281
Inclure un ID de périphérique dans les messages du journal système au format non EMBLEM 1282
Inclure la date et l'heure dans les messages du journal système 1283
Désactiver un message du journal système 1283
Modifier le niveau de gravité d'un message du journal système 1283
Bloquer les messages du journal système sur une unité de secours 1284
Inclure l'ID de périphérique dans les messages du journal système au format non EMBLEM 1284
Créer une liste d'événements personnalisée 1285
Configurer les filtres de journalisation 1286
Appliquer des filtres de message à une destination de journalisation 1286
Appliquer des filtres de journalisation 1287
Ajouter ou modifier un filtre d'ID de message du journal système 1287
Ajouter ou modifier un filtre de classe de message et de gravité 1288
Envoyer tous les messages du journal système d'une classe vers une destination de sortie spécifiée 1288
Limiter le débit de génération des messages Syslog 1289
Attribuer ou modifier des limites de débit pour les messages du journal système individuels 1290
Ajouter ou modifier la limite de débit pour un message du journal système 1290
Modifier la limite de débit pour un niveau de gravité du journal système 1290
Attribuer ou modifier des limites de débit pour la journalisation dynamique 1291
Supervision des journaux 1291
Filtrer les messages du journal système à l'aide des visionneuses de journaux 1292
Modifier les paramètres de filtrage 1294
Émettre certaines commandes à l'aide des visionneuses de journaux 1295
Historique de journalisation 1296

CHAPITRE 49 **MIB SNMP** 1299

À propos de SNMP 1299

Terminologie SNMP 1300

Présentation du SNMP version 3 1300

Modèles de sécurité 1301

SNMP Groups (groupes SNMP) 1301

Utilisateurs SNMP 1301

Hôtes SNMP 1301

Différences d'implémentation entre les logiciels ASA et Cisco IOS 1302

Messagerie du journal système SNMP 1302

Services d'application et outils tiers 1302

Lignes directrices pour SNMP 1302

Configurer SNMP 1306

Configurer une station de gestion SNMP 1306

Configurer les déroutements SNMP 1307

Configurer les paramètres pour la version 1 ou 2c du SNMP 1309

Configurer les paramètres pour la version 3 du SNMP 1310

Configurer un groupe d'utilisateurs 1312

Supervision SNMP 1313

Historique de SNMP 1314

CHAPITRE 50 **Données de télémétrie et du Cisco Success Network** 1321

À propos de Cisco Success Network 1321

Plateformes prises en charge et configurations requises 1322

Comment les données de télémétrie ASA atteignent le nuage SSE 1322

Activer ou désactiver Cisco Success Network 1322

Afficher les données de télémétrie d'ASA 1323

Cisco Success Network – Données de télémétrie 1323

CHAPITRE 51 **Alarmes pour Cisco ISA 3000** 1331

À propos des alarmes 1331

Interfaces d'entrée d'alarme. 1332

Interface de sortie d'alarme 1332

Valeurs par défaut pour les alarmes 1333
Configurer les alarmes 1333
Surveillance des alarmes 1335
Historique des alarmes 1336

CHAPITRE 52 **Rapports anonymes et Smart Call Home** 1337
À propos des rapports anonymes 1337
Exigence DNS 1338
À propos de Smart Call Home 1338
Lignes directrices relatives aux rapports anonymes et à Smart Call Home 1339
Configurer les rapports anonymes et Smart Call Home 1340
Configurer les rapports anonymes 1340
Configurer Smart Call Home 1341
Configurer l'importation automatique des certificats de groupe de confiance 1344
Supervision des rapports anonymes et de Smart Call Home 1345
Historique des rapports anonymes et de Smart Call Home 1346

PARTIE IX **Numéro de référence** 1349

CHAPITRE 53 **Adresses, protocoles et ports** 1351
Adresses IPv4 et filtres d'adresse locale 1351
Classes 1351
Réseaux privés 1352
Filtres d'adresse locale 1352
Déterminer le filtre d'adresse locale 1352
Déterminer l'adresse à utiliser avec le filtre d'adresse locale 1353
Adresses IPv6 1355
Format d'adresses IPv6 1355
Types d'adresses IPv6 1356
Adresses de monodiffusion 1356
Multicast Address (Adresse multidiffusion) 1358
Adresse Anycast 1359
Adresses requises 1360
Préfixes de l'adresse IPv6 1360

Protocoles et applications 1361
Ports TCP et UDP 1362
Ports et protocoles locaux 1365
Types ICMP 1367



À propos de ce guide

Les rubriques suivantes expliquent comment utiliser ce guide.

- Objectifs du document, à la page liii
- Documentation associée, à la page liii
- Conventions de document, à la page liii
- Communications, services et renseignements supplémentaires, à la page lv

Objectifs du document

L'objectif de ce guide est de vous aider à configurer les opérations générales de la gamme Secure Firewall ASA à l'aide de l'Adaptive Security Device Manager (ASDM). Ce guide ne couvre pas toutes les fonctionnalités, mais décrit uniquement les scénarios de configuration les plus courants.

Dans ce guide, le terme « ASA » s'applique de manière générique aux modèles pris en charge, à moins que cela ne soit spécifié autrement.

Remarque ASDM prend en charge de nombreuses versions de l'ASA. La documentation et l'aide en ligne ASDM comprennent toutes les dernières fonctionnalités prises en charge par l'ASA. Si vous utilisez une ancienne version du logiciel ASA, la documentation peut inclure des fonctionnalités qui ne sont pas prises en charge par votre version. Veuillez vous reporter au tableau de l'historique des fonctionnalités de chaque chapitre pour déterminer quand ces dernières ont été ajoutées. Pour connaître la version minimum prise en charge d'ASDM pour chaque version d'ASA, consultez *Compatibilité de la gamme Cisco ASA*.

Documentation associée

Pour en savoir plus, consultez *Parcourir la documentation de la gamme Cisco ASA* à l'adresse http://www.cisco.com/go/asadocs.

Conventions de document

Le présent document respecte les conventions de texte, d'affichage et d'alerte suivantes.

À propos de ce guide

Conventions de texte

Convention	Indication
boldface	Les commandes, les mots clés, les étiquettes de boutons, les noms de champ et le texte saisi par l'utilisateur s'affichent dans **boldface**. Pour les commandes basées sur des menus, le chemin complet vers la commande s'affiche.
italic	Les variables, pour lesquelles vous fournissez des valeurs, sont présentées dans une police de caractères en *italique*. Le type italique est également utilisé pour les titres de documents et pour l'usage général.
`monospace`	Les sessions de terminal et les renseignements affichés par le système apparaissent en police à `espacement fixe`.
{x | y | z}	Les options de mots clés obligatoires sont regroupées entre accolades et séparées par des barres verticales.
[ ]	Les éléments entre crochets sont facultatifs.
[x | y | z]	Les options de mots clés facultatifs sont regroupées entre crochets et séparées par des barres verticales.
[ ]	Les réponses par défaut aux invites du système sont également entre crochets.
< >	Les caractères qui ne s'impriment pas, tels que les mots de passe, sont délimités par des crochets en chevron.
!, #	Un point d'exclamation (!) ou un dièse (#) au début d'une ligne de code indique une ligne de commentaire.

Alertes adressées aux lecteurs

Ce document utilise les conventions suivantes pour les alertes adressées au lecteur :



Remarque Invite le *lecteur à consulter les remarques*. Les remarques contiennent des suggestions utiles ou des références à d'autres ressources non couvertes dans le manuel.



Astuces Signifie que *les renseignements suivants vous aideront à résoudre un problème.*



Mise en garde Invite le *lecteur à être prudent*. Dans cette situation, il est possible que vous effectuiez une opération risquant d'endommager l'équipement ou d'entraîner une perte de données.

Économiseur de temps	Indique que *l'action décrite permet de gagner du temps.* Vous pouvez gagner du temps en exécutant l'action décrite dans le paragraphe.
Avertissement	**Signifie que *le lecteur doit être averti.* Dans cette situation, vous pourriez effectuer une opération risquant d'entraîner des blessures corporelles.**

Communications, services et renseignements supplémentaires

- Pour recevoir des informations pertinentes et opportunes de la part de Cisco, inscrivez-vous sur le gestionnaire de profil Cisco.
- Pour obtenir les résultats commerciaux que vous recherchez avec les technologies qui comptent, visitez les services Cisco.
- Pour soumettre une demande de service, consultez le service d'assistance de Cisco.
- Pour découvrir et parcourir des applications, des produits, des solutions et des services d'entreprise sécurisés et validés, visitez Cisco MarketPlace.
- Pour obtenir des documents généraux sur la réseautique, la formation et la certification, consultez Cisco Press.
- Pour trouver des informations sur la garantie d'un produit ou d'une famille de produits particuliers, accédez à Cisco Warranty Finder.

Outil de recherche de bogues

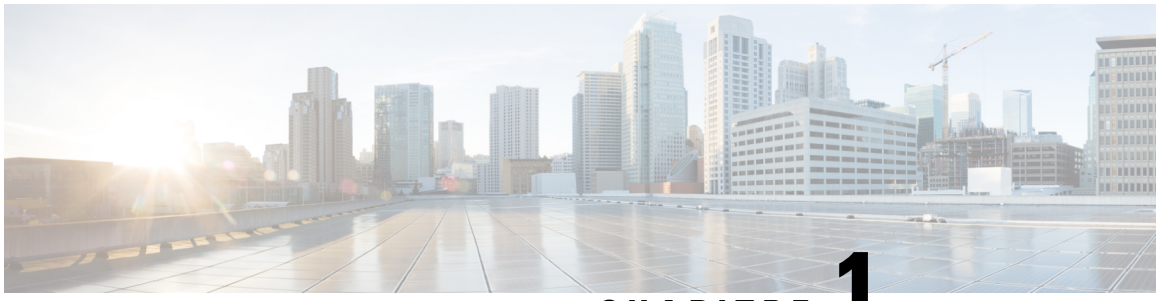
Cisco Bug Search Tool (BST) (Outil de recherche de bogues de Cisco) est un outil Web qui donne accès au système de suivi des bogues de Cisco, lequel tient à jour une liste complète des défauts et des vulnérabilités des produits et logiciels Cisco. Cet outil vous fournit des informations détaillées sur les défaillances de vos produits et logiciels.



PARTIE I

Mise en route de l'ASA

- Introduction à Secure Firewall ASA, à la page 1
- Pour commencer, à la page 17
- Interface graphique utilisateur ASDM, à la page 53
- Licences : licence à clé d'autorisation de produit pour l'ISA 3000, à la page 93
- Licences : gestion des licences logicielles Smart, à la page 125
- Périphériques logiques pour le Firepower 4100/9300, à la page 199
- Mode pare-feu transparent ou routé, à la page 219
- Assistant de démarrage, à la page 247



CHAPITRE 1

Introduction à Secure Firewall ASA

Le Secure Firewall ASA offre des fonctionnalités avancées de pare-feu dynamique et de concentrateur VPN dans un seul appareil. L'ASA comprend de nombreuses fonctionnalités avancées, comme des contextes de sécurité multiples (semblables aux pare-feu virtualisés), la mise en grappe (combinaison de plusieurs pare-feu en un seul pare-feu), les pare-feu transparents (couche 2) ou routés (couche 3), les moteurs d'inspection avancés, IPsec Prise en charge de VPN, de VPN SSL et de VPN SSL sans client et de nombreuses autres fonctionnalités.

Remarque ASDM prend en charge de nombreuses versions de l'ASA. La documentation et l'aide en ligne ASDM comprennent toutes les dernières fonctionnalités prises en charge par l'ASA. Si vous utilisez une ancienne version du logiciel ASA, la documentation peut inclure des fonctionnalités qui ne sont pas prises en charge par votre version. Veuillez vous reporter au tableau de l'historique des fonctionnalités de chaque chapitre pour déterminer quand ces dernières ont été ajoutées. Pour connaître la version minimum prise en charge d'ASDM pour chaque version d'ASA, consultez Compatibilité Cisco ASA. Consultez aussi Services spéciaux, obsolètes et existants, à la page 15.

- Exigences ASDM, à la page 1
- Compatibilité matérielle et logicielle, à la page 6
- Compatibilité VPN, à la page 6
- Nouvelles fonctionnalités, à la page 6
- Présentation fonctionnelle du pare-feu, à la page 10
- Présentation fonctionnelle VPN, à la page 14
- Présentation du contexte de sécurité, à la page 14
- Présentation de la mise en grappe d'ASA, à la page 15
- Services spéciaux, obsolètes et existants, à la page 15

Exigences ASDM

Exigences ASDM Java

Vous pouvez installer ASDM en utilisant Oracle JRE 8.0 (**asdm-*version*.bin**) ou OpenJRE 1.8.x (**asdm-openjre-*version*.bin**).

La version Oracle d'ASDM est incluse dans le forfait ASA; si vous souhaitez utiliser la version OpenJRE, vous devrez la copier sur l'ASA et le configurer pour utiliser cette version d'ASDM.



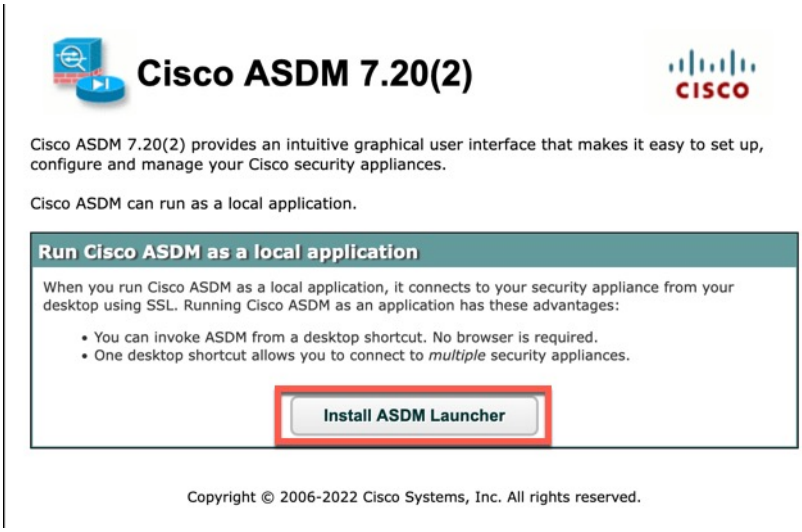
Remarque ASDM n'est pas pris en charge sur Linux.

Tableau 1 : Système d'exploitation et navigateur requis pour l'ASDM

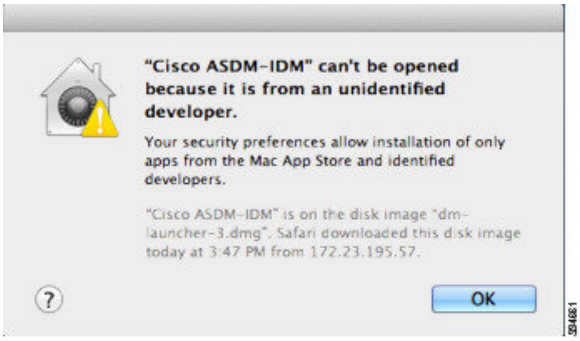
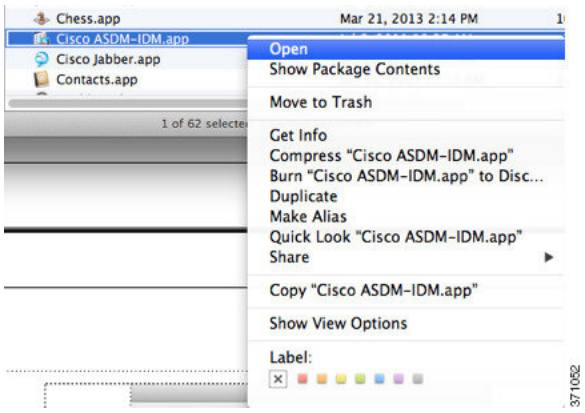
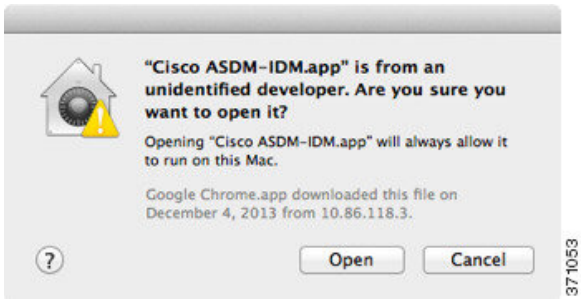
Système d'exploitation	Navigateur			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows (anglais et japonais) : • 10 **Remarque** Voir Windows 10 dans Notes de compatibilité ASDM, à la page 2 si vous avez des problèmes avec le raccourci ASDM. • 8 • 7 • Server 2016 et Server 2019 • Serveur 2012 R2 • Serveur 2012 • Serveur 2008	Oui	Aucune assistance	Oui	8.0 version 8u261 ou ultérieure	1,8 **Remarque** Aucune assistance pour Windows 7 ou 10 de 32 bits
Apple OS X 10.4 et versions ultérieures	Oui	Oui	Oui (version 64 bits uniquement)	8.0 version 8u261 ou ultérieure	1,8

Notes de compatibilité ASDM

Le tableau suivant énumère les problèmes de compatibilité avec ASDM.

Modalités	Notes
Compatibilité du lanceur ASDM avec la version d'ASDM	Message d'erreur « **Impossible de lancer le gestionnaire d'appareil** ». Si vous effectuez une mise à niveau vers une nouvelle version d'ASDM et obtenez cette erreur, vous devrez peut-être réinstaller le dernier lanceur. **1.** Ouvrez la page Web d'ASDM sur l'ASA : https://<asa_ip_address>. **2.** Cliquez sur **Installer le lanceur ASDM**. ***Illustration 1 : Installer le lanceur ASDM***  **3.** Laissez les champs du nom d'utilisateur et du mot de passe vides (pour une nouvelle installation), puis cliquez sur **OK**. En l'absence d'authentification HTTPS, vous pouvez accéder à ASDM sans nom d'utilisateur et mot de passe **d'activation**, qui est vide par défaut. Lorsque vous saisissez la commande **enable** au niveau de l'interface de ligne de commande pour la première fois, vous êtes invité à modifier le mot de passe; ce comportement n'est pas appliqué lorsque vous vous connectez à ASDM. Nous vous suggérons de modifier le mot de passe d'activation dès que possible afin qu'il ne reste pas vide. **Remarque** : Si vous avez activé l'authentification HTTPS, saisissez votre nom d'utilisateur et le mot de passe associé. Même sans authentification, si vous saisissez un nom d'utilisateur et un mot de passe à l'écran de connexion (au lieu de laisser le nom d'utilisateur vide), ASDM vérifie la base de données locale à la recherche d'une correspondance.

Modalités	Notes
Accès à l'annuaire Windows Active Directory	Dans certains cas, les paramètres Active Directory pour les utilisateurs Windows peuvent restreindre l'accès aux emplacements des fichiers de programme nécessaires pour lancer ASDM sur Windows. L'accès aux répertoires suivants est nécessaire : • Dossier du bureau • C:\Windows\System32C:\Users\<username>\.asdm • C:\Program Files (x86)\Cisco Systems Si votre Active Directory restreint l'accès à l'annuaire, vous devez demander l'accès à votre administrateur Active Directory.
Windows 10	Message d'erreur « **This app can't run on your PC** » (cette application ne peut pas fonctionner sur votre ordinateur personnel). Lorsque vous installez le lanceur ASDM, Windows 10 peut remplacer la cible du raccourci ASDM par le chemin de l'hôte Windows Scripting, ce qui provoque cette erreur. Pour fixer la cible du raccourci : **1.** Choisissez **Start (Démarrer)** > **Cisco ASDM-IDM Launcher (lanceur Cisco ASDM-IDM)** , et cliquez avec le bouton droit de la souris sur l'application **Cisco ASDM-IDM Launcher** (lanceur Cisco ASDM-IDM). **2.** Choisissez **More** > **Open file location** (Plus > Ouvrir l'emplacement du fichier.) Windows ouvre le répertoire avec l'icône du raccourci. **3.** Cliquez avec le bouton droit de la souris sur l'icône du raccourci et choisissez **Properties** (propriétés). **4.** Modifier la **Target** (cible) en : **C:\Windows\System32\wscript.exe invisible.vbs run.bat** **5.** Cliquez sur **OK**.
OS X	Sous OS X, vous pouvez être invité à installer Java la première fois que vous lancez ASDM; suivez les instructions si nécessaire. ASDM sera lancé une fois l'installation terminée.

Modalités	Notes
OS X 10.8 et versions ultérieures	Vous devez autoriser l'exécution d'ASDM, car il n'est pas signé avec un identifiant du développeur Apple. Si vous ne modifiez pas vos préférences de sécurité, un écran d'erreur s'affiche.  1. Pour permettre à ASDM de s'exécuter, faites un clic droit (ou Ctrl-Clic) sur l'icône du lanceur Cisco ASDM-IDM, et choisissez **Open** (ouvrir).  2. Un écran d'erreur similaire s'affiche, mais vous pouvez ouvrir ASDM à partir de cet écran. Cliquez sur **Open** (ouvrir) Le lanceur ASDM-IDM s'ouvre. 

Modalités	Notes
(ASA 5500 et ISA 3000) Requiert une licence de chiffrement fort (3DES/AES) sur l'ASA **Remarque** Les modèles de licence intelligents permettent un accès à ASDM sans la licence à chiffrement fort.	ASDM nécessite une connexion SSL avec l'ASA. Vous pouvez demander une licence 3DES PAK à Cisco : **1.** Accédez à l'adresse https://www.cisco.com/go/license. **2.** Sous **Licences traditionnelles**, cliquez sur **Accès LRP**. **3.** Cliquez sur **Obtenir des licences**, puis choisissez **IPS, Crypto, Autre…** dans la liste déroulante. **4.** Tapez **ASA** dans le champ **Search by Keyword** (Recherche par mot clé). **5.** Sélectionnez **Cisco ASA 3DES/AES License** (licence Cisco ASA 3DES/AES) dans la liste **Product** (produit), puis cliquez sur **Next** (suivant). **6.** Saisissez le numéro de série de l'ASA et suivez les invites pour demander une licence 3DES/AES pour l'ASA.
• Certificat auto-signé ou certificat non fiable • IPv6 • Firefox et Safari	Lorsque l'ASA utilise un certificat auto-signé ou un certificat non fiable, Firefox et Safari ne peuvent pas ajouter d'exceptions de sécurité lors de la navigation avec HTTPS sur IPv6. Voir https://bugzilla.mozilla.org/show_bug.cgi?id=633001. Cette mise en garde concerne toutes les connexions SSL provenant de Firefox ou Safari vers l'ASA (y compris les connexions ASDM). Pour éviter cet inconvénient, configurez un certificat approprié pour l'ASA, délivré par une autorité de certification de confiance.
• Le chiffrement SSL sur l'ASA doit inclure à la fois RC4-MD5 et RC4-SHA1 ou désactiver le faux départ SSL dans Chrome. • Chrome	Si vous changez le chiffrement SSL sur l'ASA pour exclure les algorithmes RC4-MD5 et RC4-SHA1 (ces algorithmes sont activés par défaut), Chrome ne peut pas lancer ASDM à cause de la fonction « SSL false start » de Chrome. Nous suggérons de réactiver l'un de ces algorithmes (voir le volet **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSL Settings (Paramètres SSL)**) ou vous pouvez désactiver le faux départ de SSL dans Chrome en utilisant l'indicateur **--disable-ssl-false-start** conformément à Exécuter Chrome avec des indicateurs.

Compatibilité matérielle et logicielle

Pour obtenir la liste complète du matériel et des logiciels pris en charge, consultez la section Compatibilité Cisco ASA.

Compatibilité VPN

Consultez Plateformes VPN prises en charge, série Cisco ASA.

Nouvelles fonctionnalités

Cette section énumère les nouvelles fonctionnalités de chaque version.

Remarque Les messages syslog nouveaux, modifiés et obsolètes sont répertoriés dans le guide des messages syslog.

Nouvelles fonctionnalités dans ASDM 7.19(1.95)

Publication : 5 juillet 2023

Il n'y a pas de nouvelles fonctionnalités dans cette version.

Nouvelles fonctionnalités dans ASDM 7.19(1.90)

Date de sortie : 16 février 2023

Il n'y a pas de nouvelles fonctionnalités dans cette version.

Nouvelles fonctionnalités dans l'ASA 9.19(1)/ASDM 7.19(1)

Publication : 29 novembre 2022

Fonctionnalités	Description
Caractéristiques de la plateforme	
Secure Firewall 3105	Nous avons présenté l'ASA pour le Secure Firewall 3105.
Solution virtuelle ASA Auto Scale avec équilibreur de charge de la passerelle Azure	Vous pouvez maintenant déployer la solution virtuelle ASA Auto Scale avec équilibreur de charge de la passerelle sur Microsoft Azure. Consultez les fonctionnalités Interfaces pour en savoir plus.
Caractéristiques du pare-feu	
Soutien aux groupes de service du réseau	Vous pouvez désormais définir un maximum de 1 024 groupes de services réseau.
Fonctionnalités de haute disponibilité et d'évolutivité	
Suppression des propos tendancieux	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
Regroupement virtuel d'ASA sur Amazon Web Services (AWS)	L'ASA virtuel prend en charge le regroupement d'interfaces individuelles pour un maximum de 16 nœuds sur AWS. Vous pouvez utiliser la mise en grappe avec ou sans équilibreur de charge de la passerelle AWS. ASDM n'est pas pris en charge.

Fonctionnalités	Description
Fonctionnalités de routage	
Prise en charge du redémarrage progressif de BGP pour IPv6	Nous avons ajouté la prise en charge du redémarrage progressif de BGP pour la famille d'adresses IPv6. Écrans nouveaux/modifiés : **Configuration** > **Configuration de l'appareil** > **Routage** > **BGP** > **Famille IPv6** > **Voisin**.
Prise en charge par ASDM des interfaces de bouclage pour le trafic BGP	ASDM prend en charge maintenant la configuration d'une interface avec boucle avec retour comme interface source pour le voisinage BGP. L'interface de bouclage permet de surmonter les défaillances du chemin. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Routing (routage)** > **BGP** > **IPv4 Family / IPv6 Family (famille IPv4 / famille IPv6)** > **Neighbor (voisin)** > **Add (ajouter)** > **General (général)**.
Caractéristiques de l'interface	
Prise en charge virtuelle de l'IPv6 par l'ASA	ASAv pour prendre en charge le protocole réseau IPv6 sur les plateformes du nuage privé et public. Les utilisateurs peuvent désormais : • Activer et configurer une adresse de gestion IPv6 via la configuration day0. • Attribuer des adresses IPv6 à l'aide de méthodes DHCP et statiques.
Proxy jumelé VXLAN pour l'ASA virtuel pour l'équilibreur de charges de la passerelle Azure.	Vous pouvez configurer une interface VXLAN en mode proxy apparié pour l'ASA virtuel dans Azure afin de l'utiliser avec l'équilibreur de charges de la passerelle Azure (GWLB). L'ASA virtuel définit une interface externe et une interface interne sur un seul NIC en utilisant des segments VXLAN dans un serveur mandataire jumelé. Commandes nouvelles/modifiées : **port externe, segment-id externe, port interne, segment-id interne, proxy paired** ASDM n'est pas pris en charge.
La correction d'erreur par défaut (FEC) sur les ports fixes du Secure Firewall 3100 est passée de cl74-fc à cl108-rs pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+.	Lorsque vous définissez le FEC sur Auto sur les ports fixes du Secure Firewall 3100, le type par défaut est désormais défini sur cl108-rs au lieu de cl74-fc pour les émetteurs-récepteurs SR, CSR et LR de 25 Go. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Edit Interface (éditer l'interface)** > **Configure Hardware Properties (configurer les propriétés du matériel)** > **FEC Mode (mode FEC)**
Prise en charge par ASDM des interfaces de bouclage	ASDM prend désormais en charge les interfaces de bouclage. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add Loopback Interface (ajouter une interface de bouclage)**.
Caractéristiques de la licence	

Fonctionnalités	Description
Prise en charge de la réservation de licences virtuelles permanentes pour l'ASAv5 sur KVM et VMware	Une nouvelle commande est disponible que vous pouvez exécuter pour remplacer la licence DPP par défaut et demander à Cisco Smart Software Manager (SSM) d'envoyer une licence DPP ASAv5 lorsque vous déployez ASAv avec 2GB RAM sur KVM et VMware. Vous pouvez modifier la même commande en ajoutant la forme <*no*> pour rétablir la licence de l'ASAv5 à la licence DPP par défaut en fonction de la configuration de la mémoire vive.
Fonctions d'administration, de surveillance et de dépannage	
Pile CiscoSSH maintenant par défaut	La pile Cisco SSH est maintenant utilisée par défaut. Écrans Nouveaux ou modifiés : • Mode de contexte unique : **Configuration** > **Device Management (Gestion des appareils)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** • Mode de contexte multiple : **Configuration** > **Device Management (Gestion des appareils)** > **SSH Stack (Pile SSH)**
Fonctionnalités du VPN	
Prise en charge de l'interface de bouclage VTI	Vous pouvez désormais définir une interface de bouclage comme interface source pour un VTI. La possibilité d'hériter de l'adresse IP d'une interface de bouclage au lieu d'une adresse IP configurée de manière statique a également été ajoutée. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP attribuée à l'interface de boucle avec retour. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add VTI Interface (ajouter une interface VTI)** > **Advanced (avancé)**.
Prise en charge de l'interface de tunnel virtuel dynamique (VTI dynamique)	L'ASA est amélioré grâce à l'ITV dynamique. Un seul VTI dynamique peut remplacer plusieurs configurations de VTI statique sur le concentrateur. Vous pouvez ajouter de nouveaux satellites à un concentrateur sans modifier la configuration du concentrateur. Dynamique VTI prend en charge les rayons dynamiques (DHCP). Écrans nouveaux/modifiés : **Configuration > Device Setup > Interface Settings > Interfaces > Add > DVTI Interface**
Support VTI pour EIGRP et OSPF	Le routage EIGRP et OSPFv2/v3 est désormais pris en charge sur l'interface du tunnel virtuel. Vous pouvez maintenant utiliser ces protocoles de routage pour partager les informations de routage et pour acheminer le flux de trafic à travers le tunnel VPN basé sur VTI entre les pairs.

Fonctionnalités	Description
TLS 1.3 dans le VPN d'accès à distance	Vous pouvez désormais utiliser TLS 1.3 pour chiffrer les connexions VPN d'accès à distance. TLS 1.3 ajoute la prise en charge des chiffrements suivants : • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 Cette fonctionnalité nécessite Cisco Secure Client, version 5.0.01242 ou ultérieure. Écrans nouveaux/modifiés : **Configuration > Device Management > Advanced > SSL Settings (Configuration > Gestion des appareils > Avancé > Paramètres SSL)**
Prise en charge de la double pile pour les clients tiers IKEv2	Secure Firewall ASA prend désormais en charge les demandes d'IP à double pile provenant de clients VPN d'accès à distance tiers IKEv2. Si le client VPN d'accès à distance tiers demande des adresses IPv4 et IPv6, l'ASA peut désormais attribuer les deux versions d'adresses IP à l'aide de plusieurs sélecteurs de trafic. Cette fonction permet aux clients VPN d'accès à distance tiers d'envoyer des données IPv4 et IPv6 par le biais d'un seul tunnel IPsec.
Sélecteur de trafic pour l'interface VTI statique	Vous pouvez maintenant attribuer un sélecteur de trafic à une interface VTI statique.
Spécifier la version maximum du protocole SSL/TLS	Vous pouvez désormais spécifier la version maximum du protocole SSL/TLS que l'ASA peut utiliser en tant que client ou serveur.

Présentation fonctionnelle du pare-feu

Les pare-feu protègent les réseaux internes contre les accès non autorisés par des utilisateurs d'un réseau externe. Un pare-feu peut également protéger les réseaux internes les uns des autres, par exemple en séparant le réseau des ressources humaines du réseau des utilisateurs. Si vous avez des ressources réseau qui doivent être disponibles pour un utilisateur externe, comme un serveur Web ou FTP, vous pouvez placer ces ressources sur un réseau distinct derrière le pare-feu, appelé *zone démilitarisée* (DMZ). Le pare-feu permet un accès limité à la DMZ, mais comme celle-ci ne comprend que les serveurs publics, une attaque à cet endroit n'affecte que les serveurs et n'affecte pas les autres réseaux internes. Vous pouvez également contrôler quand les utilisateurs internes accèdent aux réseaux externes (par exemple, l'accès à Internet), en n'autorisant que certaines adresses, en exigeant une authentification ou une autorisation, ou en effectuant une coordination avec un serveur de filtrage d'URL externe.

Lorsqu'il est question de réseaux connectés à un pare-feu, le réseau *externe* se trouve devant le pare-feu, le réseau *interne* est protégé et se trouve derrière le pare-feu, et une *DMZ*, bien que située derrière le pare-feu, permet un accès limité aux utilisateurs externes. Étant donné que l'ASA vous permet de configurer de nombreuses interfaces avec des politiques de sécurité variées, y compris de nombreuses interfaces internes, de nombreuses DMZ et même de nombreuses interfaces externes si vous le souhaitez, ces termes sont utilisés dans un sens général uniquement.

Présentation de la politique de sécurité

Une politique de sécurité détermine quel trafic est autorisé à traverser le pare-feu pour accéder à un autre réseau. Par défaut, l'ASA permet au trafic de circuler librement d'un réseau interne (niveau de sécurité supérieur) vers un réseau externe (niveau de sécurité inférieur). Vous pouvez appliquer des actions au trafic pour personnaliser la politique de sécurité.

Autorisation ou refus de trafic avec critères d'accès

Vous pouvez appliquer des critères d'accès pour limiter le trafic de l'intérieur vers l'extérieur ou autoriser le trafic de l'extérieur vers l'intérieur. Pour les interfaces de groupe de ponts, vous pouvez également appliquer un critère d'accès EtherType pour autoriser le trafic non IP.

Application de la NAT

Voici quelques avantages de la NAT :

- Vous pouvez utiliser des adresses privées sur vos réseaux internes. Les adresses privées ne sont pas routables sur Internet.
- La NAT masque les adresses locales des autres réseaux afin que les agresseurs ne puissent pas découvrir l'adresse réelle d'un hôte.
- La NAT peut résoudre les problèmes de routage IP en prenant en charge le chevauchement des adresses IP.

Protection contre les fragments IP

L'ASA fournit une protection contre les fragments d'adresse IP. Cette fonctionnalité effectue le réassemblage complet de tous les messages d'erreur ICMP et le réassemblage virtuel des fragments IP restants qui sont acheminés par l'ASA. Les fragments qui échouent à la vérification de sécurité sont abandonnés et enregistrés. Le réassemblage virtuel ne peut pas être désactivé.

Application du filtrage HTTP, HTTPS ou FTP

Bien que vous puissiez utiliser des listes d'accès pour empêcher l'accès sortant à des sites Web ou à des serveurs FTP spécifiques, la configuration et la gestion de l'utilisation du Web de cette manière ne sont pas pratiques en raison de la taille et de la nature dynamique d'Internet.

Vous pouvez configurer les fonctionnalités de sécurisation du web sur l'ASA. Vous pouvez également utiliser l'ASA en conjonction avec un produit externe tel que l'appliance Cisco pour la sécurité du web (WSA).

Application de l'inspection des applications

Des plateformes d'inspection sont nécessaires pour les services qui intègrent des renseignements d'adressage IP dans le paquet de données des utilisateurs ou qui ouvrent des canaux secondaires sur des ports attribués de manière dynamique. Ces protocoles exigent que l'ASA effectue une inspection approfondie des paquets.

Application des politiques de QoS

Certains trafics réseau, comme les messages vocaux et le streaming vidéo, ne peuvent pas tolérer de longs temps de latence. La QoS est une fonctionnalité réseau qui vous permet de donner la priorité à ces types de trafic. La QoS renvoie à la capacité d'un réseau à fournir un meilleur service au trafic réseau sélectionné.

Application des limites de connexion et de la normalisation TCP

Vous pouvez limiter les connexions TCP et UDP ainsi que les connexions amorces. La limitation du nombre de connexions et de connexions amorces vous protège contre les attaques DoS. L'ASA utilise la limite amorce pour déclencher l'interception TCP, qui protège les systèmes internes contre une attaque DoS perpétrée en inondant une interface de paquets SYN de TCP. Une connexion amorce est une demande de connexion qui n'a pas terminé l'établissement de liaison entre la source et la destination.

La normalisation TCP est une fonctionnalité composée de paramètres de connexion TCP avancés conçus pour abandonner les paquets qui n'apparaissent pas normaux.

Activation de la détection des menaces

Vous pouvez configurer la détection des menaces par analyse et la détection des menaces de base, ainsi que l'utilisation des statistiques pour analyser les menaces.

La détection des menaces de base détecte les activités qui peuvent être liées à une attaque, comme les attaques DoS, et envoie automatiquement un message de journal système.

Une attaque par analyse typique se compose d'un hôte qui teste l'accessibilité de chaque adresse IP d'un sous-réseau (en analysant de nombreux hôtes dans le sous-réseau ou en balayage de nombreux ports dans un hôte ou un sous-réseau). La fonction de détection des menaces par analyse détermine quand un hôte effectue une analyse. Contrairement à la détection d'analyse IPS qui est basée sur les signatures de trafic, la fonction de détection des menaces par analyse ASA gère une base de données étendue qui contient des statistiques d'hôte pouvant être analysées pour l'activité d'analyse.

La base de données d'hôtes suit les activités suspectes telles que les connexions sans activité de retour, l'accès à des ports de service fermés, les comportements TCP vulnérables tels que les IPID non aléatoires, etc.

Vous pouvez configurer l'ASA pour envoyer des messages de journal système sur un agresseur ou vous pouvez automatiquement l'hôte.

Présentation du mode pare-feu

L'ASA fonctionne dans deux modes de pare-feu différents :

- Acheminé
- Transparent

En mode routage, l'ASA est considéré comme un saut de routeur dans le réseau.

En mode transparent, l'ASA agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et n'est pas considéré comme un saut de routeur. L'ASA se connecte au même réseau sur ses interfaces interne et externe dans un « groupe de ponts ».

Vous pouvez utiliser un pare-feu transparent pour simplifier la configuration de votre réseau. Le mode transparent est également utile si vous souhaitez que le pare-feu soit visible par les agresseurs. Vous pouvez également utiliser un pare-feu transparent pour le trafic qui serait autrement bloqué en mode routé. Par exemple, un pare-feu transparent peut autoriser les flux de multidiffusion à l'aide d'une liste d'accès EtherType.

Le mode routé prend en charge le routage et le pont intégré. Vous pouvez donc également configurer des groupes de ponts en mode routé et acheminer le routage entre les groupes de ponts et les interfaces normales. En mode routé, vous pouvez répliquer la fonctionnalité en mode transparent; si vous n'avez pas besoin du mode de contexte multiple ou de la mise en grappe, vous pouvez envisager d'utiliser le mode routé.

Présentation de l'inspection dynamique

Tout le trafic qui passe par l'ASA est inspecté à l'aide de l'algorithme de sécurité adaptatif et est autorisé ou abandonné. Un filtre de paquet simple peut vérifier l'adresse source, l'adresse de destination et les ports appropriés, mais il ne vérifie pas si la séquence ou les indicateurs des paquets sont corrects. Un filtre vérifie également *chaque* paquet par rapport au filtre, ce qui peut être un processus lent.



Remarque La fonction de contournement d'état TCP vous permet de personnaliser le flux de paquet.

Cependant, un pare-feu dynamique comme l'ASA prend en compte l'état d'un paquet :

- S'agit-il d'une nouvelle connexion?

  S'il s'agit d'une nouvelle connexion, l'ASA doit vérifier le paquet par rapport aux listes d'accès et effectuer d'autres tâches pour déterminer si le paquet est autorisé ou refusé. Pour effectuer cette vérification, le premier paquet de la session passe par le « chemin de gestion de session » et, selon le type de trafic, il peut également passer par le « chemin de plan de commande ».

  Le chemin de gestion de session est responsable des tâches suivantes :

  - Effectuer les vérifications de la liste d'accès
  - Effectuer des recherches de route
  - Attribuer des traductions NAT (xlates)
  - Établir des sessions dans le « chemin rapide »

  L'ASA crée des flux de transfert et d'inversion dans le chemin rapide pour le trafic TCP; l'ASA crée également des renseignements sur l'état de connexion pour les protocoles sans connexion comme UDP et ICMP (lorsque vous activez l'inspection ICMP), afin qu'ils puissent également utiliser le chemin rapide.



Remarque Pour les autres protocoles IP, comme SCTP, l'ASA ne crée pas de flux de chemin inverse. Par conséquent, les paquets d'erreur ICMP qui font référence à ces connexions sont abandonnés.

  Certains paquets nécessitant une inspection de couche 7 (la charge utile des paquets doit être inspectée ou modifiée) sont transmis au chemin du plan de commande. Des moteurs d'inspection de couche 7 sont nécessaires pour les protocoles qui ont au moins deux canaux : un canal de données, qui utilise des numéros de port connus, et un canal de contrôle, qui utilise des numéros de port différents pour chaque session. Ces protocoles comprennent FTP, H.323 et SNMP.

- S'agit-il d'une connexion établie?

  Si la connexion est déjà établie, l'ASA n'a pas besoin de revérifier les paquets; la plupart des paquets correspondants peuvent passer par le chemin « rapide » dans les deux sens. Le chemin rapide est responsable des tâches suivantes :

  - Vérification de la somme de contrôle IP
  - Recherche de session

- Vérification du numéros de séquence TCP
- Traductions NAT en fonction des sessions existantes
- Ajustements des en-têtes de couche 3 et 4

Les paquets de données pour les protocoles qui nécessitent une inspection de couche 7 peuvent également passer par le chemin rapide.

Certains paquets de session établis doivent continuer à emprunter le chemin de gestion de session ou le chemin du plan de commande. Les paquets qui empruntent le chemin de gestion de session comprennent les paquets HTTP qui nécessitent une inspection ou un filtrage de contenu. Les paquets qui empruntent le chemin du plan de commande comprennent les paquets de contrôle pour les protocoles qui nécessitent une inspection de couche 7.

Présentation fonctionnelle VPN

Un VPN est une connexion sécurisée sur un réseau TCP/IP (tel qu'Internet) qui s'affiche comme une connexion privée. Cette connexion sécurisée s'appelle un tunnel. L'ASA utilise des protocoles de tunnellisation pour négocier les paramètres de sécurité, créer et gérer des tunnels, encapsuler des paquets, transmettre ou recevoir des paquets par le tunnel et les désencapsuler. L'ASA fonctionne comme un point terminal de tunnel bidirectionnel : il peut recevoir des paquets simples, les encapsuler et les envoyer à l'autre extrémité du tunnel où ils sont désencapsulés et envoyés à leur destination finale. Il peut également recevoir des paquets encapsulés, les désencapsuler et les envoyer à leur destination finale. L'ASA invoque divers protocoles standard pour remplir ces fonctions.

L'ASA remplit les fonctions suivantes :

- Établit des tunnels
- Négocie les paramètres du tunnel
- Authentifie les utilisateurs
- Attribue des adresses d'utilisateur
- Chiffre et déchiffre les données
- Gère les clés de sécurité
- Gère le transfert de données dans le tunnel
- Gère le transfert de données entrant et sortant en tant que point terminal de tunnel ou routeur

L'ASA invoque divers protocoles standard pour remplir ces fonctions.

Présentation du contexte de sécurité

Vous pouvez partitionner un ASA unique en plusieurs périphériques virtuels, appelés contextes de sécurité. Chaque contexte de sécurité est un périphérique indépendant, avec sa politique de sécurité, ses interfaces et ses administrateurs. Les contextes multiples sont similaires au fait d'avoir plusieurs périphériques autonomes. De nombreuses fonctionnalités sont prises en charge en mode de contexte multiple, notamment les tables de

routage, les fonctionnalités de pare-feu, IPS et la gestion; cependant, certaines fonctionnalités ne sont pas prises en charge. Consultez les chapitres consacrés aux fonctionnalités pour en savoir plus.

En mode de contexte multiple, l'ASA comprend une configuration pour chaque contexte qui identifie la politique de sécurité, les interfaces et presque toutes les options que vous pouvez configurer sur un périphérique autonome. L'administrateur système ajoute et gère les contextes en les configurant dans la configuration système, qui, à l'instar d'une configuration monomode, est la configuration de démarrage. La configuration système identifie les paramètres de base de l'ASA. La configuration système n'inclut aucune interface réseau ni aucun paramètre réseau pour elle-même; au contraire, lorsque le système doit accéder à des ressources réseau (comme le téléchargement des contextes à partir du serveur), il utilise l'un des contextes désigné comme contexte d'administration.

Le contexte d'administration est comme un contexte de sécurité, sauf que lorsqu'un utilisateur se connecte au contexte d'administration, cet utilisateur dispose de droits d'administrateur système et peut accéder au système et à tous les autres contextes.

Présentation de la mise en grappe d'ASA

La mise en grappe d'ASA vous permet de regrouper plusieurs ASA en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques.

Vous effectuez toute la configuration (à l'exception de la configuration de démarrage) sur l'unité de contrôle uniquement; la configuration est ensuite répliquée sur les unités membres.

Services spéciaux, obsolètes et existants

Pour certains services, la documentation se trouve en dehors des guides de configuration principaux et de l'aide en ligne.

Guides de services spéciaux

Des services spéciaux permettent à l'ASA d'interagir avec d'autres produits Cisco; par exemple, en fournissant un mandataire de sécurité pour les services téléphoniques (Unified Communications), en fournissant le filtrage du trafic réseau de zombies en conjonction avec la base de données dynamique du serveur de mise à jour de Cisco, ou en fournissant des services WCCP pour l'appliance Cisco pour la sécurité du web. Certains de ces services spéciaux sont couverts par des guides distincts :

- Guide de filtrage du trafic du réseau de zombies Cisco ASA
- Guide de mise en œuvre de Cisco ASA NetFlow
- Guide de Cisco ASA Unified Communications
- Guide de redirection du trafic WCCP Cisco ASA
- Guide de mise en œuvre des outils SNMP version 3

Services obsolètes

Pour les fonctionnalités obsolètes, consultez le guide de configuration de votre version ASA. De même, pour les fonctionnalités repensées telles que la NAT entre les versions 8.2 et 8.3 ou les interfaces en mode transparent entre les versions 8.3 et 8.4, consultez le guide de configuration de votre version. Bien

qu'ASDM soit rétrocompatible avec les versions ASA précédentes, le guide de configuration et l'aide en ligne ne couvrent que la dernière version.

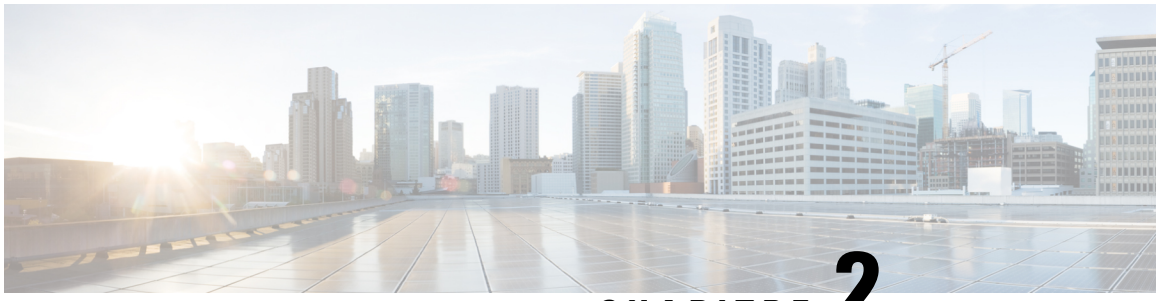
Guide des services existants

Les services existants sont toujours pris en charge sur l'ASA, mais il peut y avoir de meilleurs services de remplacement que vous pouvez utiliser à la place. Les services existants sont couverts dans un guide distinct :

Guide des fonctionnalités existantes de Cisco ASA

Ce guide comprend les chapitres suivants :

- Configuration de RIP
- Règles AAA pour l'accès au réseau
- À l'aide des outils de protection, qui comprennent la prévention de l'usurpation d'adresse IP (**ip verify reverse-path**), la configuration de la taille des fragments (**fragment**), le blocage des connexions indésirables (**shun**), la configuration des options TCP (pour ASDM) et la configuration de l'audit IP pour la prise en charge IPS de base (**ip audit**).
- Configuration des services de filtrage



CHAPITRE 2

Pour commencer

Ce chapitre décrit comment démarrer l'utilisation de votre ASA.

- Accéder à la console de l'interface de commande en ligne, à la page 17
- Activer le mode FIPS, à la page 24
- Configurer l'accès ASDM, à la page 25
- Démarrer ASDM, à la page 28
- Personnaliser le fonctionnement ASDM, à la page 30
- Configurations d'usine par défaut, à la page 32
- Régler le Firepower 2100 en mode appareil ou plateforme, à la page 47
- Commencer avec la configuration, à la page 49
- Utiliser l'outil d'interface de ligne de commande dans ASDM, à la page 50
- Appliquer les modifications de configuration aux connexions, à la page 51

Accéder à la console de l'interface de commande en ligne

Dans certains cas, vous devrez peut-être utiliser l'interface de ligne de commande pour configurer les paramètres de base pour l'accès à ASDM.

Pour la configuration initiale, accédez à l'interface de ligne de commande directement à partir du port de console. Plus tard, vous pourrez configurer l'accès à distance à l'aide de Telnet ou SSH conformément à Accès de gestion, à la page 1135. Si votre système est déjà en mode de contexte multiple, l'accès au port de console vous place dans l'espace d'exécution du système.

Si vous obtenez des caractères non lisibles lors de la connexion au port de console, vérifiez les paramètres du port. S'ils sont corrects, essayez le câble avec un autre appareil en utilisant les mêmes paramètres. Si le câble est en bon état, vous devrez peut-être remplacer le matériel du port de console. Envisagez également d'essayer un autre ordinateur de travail pour établir la connexion.

Remarque Pour l'accès à la console ASA virtuel, consultez le guide de démarrage rapide ASA virtuel.

Accéder à la console de l'ISA 3000

Procédez comme suit pour accéder à la console de l'appareil.

Procédure

Étape 1 Connectez un ordinateur au port de la console à l'aide du câble de console fourni, puis connectez-vous à la console à l'aide d'un émulateur de terminal pour 9600 bauds, 8 bits de données, aucune parité, 1 bit d'arrêt, aucun contrôle de flux.

Pour plus de renseignements sur le câble de console, consultez le guide sur le matériel pour votre ASA.

Étape 2 Appuyez sur la touche **Entrée** pour afficher l'invite suivante :

```
ciscoasa>
```

Cette invite indique que vous êtes en mode EXEC utilisateur. Le mode EXEC utilisateur donne uniquement accès aux commandes de base.

Étape 3 Accédez au mode d'exécution privilégié.

enable

Vous êtes invité à en changer le mot de passe la première fois que vous entrez la commande **enable**.

Exemple :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

Toutes les commandes non liées à la configuration sont disponibles en mode d'exécution privilégié. Vous pouvez également passer en mode de configuration à partir du mode d'exécution privilégié.

Pour quitter le mode privilégié, entrez la commande **disable**, **exit** ou **quit** .

Étape 4 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Vous pouvez commencer à configurer l'ASA à partir du mode de configuration globale. Pour quitter le mode de configuration globale, entrez la commande **exit**, **quit** ou **end**.

Accéder à la console du mode plateforme de Firepower 2100

Le port de console Firepower 2100 se connecte à l'interface de ligne de commande de Secure Firewall eXtensible Operating System (interface de ligne de commande de FXOS). À partir de l'interface de ligne de

commande de FXOS, vous pouvez ensuite vous connecter à la console ASA, puis revenir en arrière. Si vous établissez un lien entre SSH et FXOS, vous pouvez également vous connecter à l'interface de ligne de commande d'ASA; une connexion SSH n'est pas une connexion de console, vous pouvez donc avoir plusieurs connexions ASA à partir d'une connexion SSH FXOS. De même, si vous vous connectez à l'ASA, vous pouvez vous connecter à l'interface de ligne de commande de FXOS.

Avant de commencer

Vous ne pouvez avoir qu'une seule connexion de console à la fois. Lorsque vous vous connectez à la console ASA à partir de la console FXOS, cette connexion est une connexion de console persistante, différente d'une connexion Telnet ou SSH.

Procédure

Étape 1 Connectez votre ordinateur de gestion au port de console. Firepower 2100 est livrée avec un câble série DB-9 à RJ-45, vous aurez donc besoin d'un câble série USB tiers pour établir la connexion. Assurez-vous d'installer les pilotes série USB nécessaires à votre système d'exploitation. Utilisez les paramètres de série suivants :

- 9 600 bauds
- 8 bits de données
- Pas de parité
- 1 bit d'arrêt

Vous vous connectez à l'interface de ligne de commande FXOS. Entrez les informations d'identification de l'utilisateur; par défaut, vous pouvez vous connecter avec l'utilisateur **admin** et le mot de passe par défaut, **Admin123**.

Étape 2 Connectez-vous à l'ASA :

connect asa

Exemple :

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

Étape 3 Accédez au mode d'exécution privilégié.

enable

Lors de votre première saisie de la commande **enable**, vous devrez modifier le mot de passe.

Exemple :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

Toutes les commandes non liées à la configuration sont disponibles en mode d'exécution privilégié. Vous pouvez également passer en mode de configuration à partir du mode d'exécution privilégié.

Pour quitter le mode privilégié, entrez la commande **disable**, **exit** ou **quit** .

Étape 4 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Vous pouvez commencer à configurer l'ASA à partir du mode de configuration globale. Pour quitter le mode de configuration globale, entrez la commande **exit**, **quit** ou **end**.

Étape 5 Pour revenir à la console FXOS, entrez **Ctrl+a**, **d**.

Étape 6 Si vous vous connectez à l'aide du protocole SSH à l'ASA (après avoir configuré l'accès SSH sur l'ASA), connectez-vous à l'interface de ligne de commande de FXOS.

connect fxos

Vous serez invité à vous authentifier pour accéder à FXOS. Utilisez le nom d'utilisateur : **admin** et le mot de passe : **Admin123** par défaut. Pour revenir à l'interface de ligne de commande de l'ASA, entrez **exit** ou tapez **Ctrl-Shift-6**, **x**.

Exemple :

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Accès à la console Firepower 1000, 2100 en mode appareil et Secure Firewall 3100

Le port de console des Firepower 1000, 2100 en mode appareil et Secure Firewall 3100 vous relie à l'interface de ligne de commande de l'ASA (contrairement à la console Firepower 2100 en mode plateforme, qui vous relie à l'interface de ligne de commande FXOS). À partir de l'interface de ligne de commande d'ASA, vous pouvez ensuite vous connecter à l'interface de ligne de commande FXOS à l'aide de Telnet à des fins de dépannage.

Procédure

Étape 1 Connectez votre ordinateur de gestion au port de console. Assurez-vous d'installer les pilotes série nécessaires à votre système d'exploitation. Utilisez les paramètres de série suivants :

- 9 600 bauds
- 8 bits de données
- Pas de parité
- 1 bit d'arrêt

Vous vous connectez à l'interface de ligne de commande d'ASA. Aucun identifiant d'utilisateur n'est requis pour l'accès à la console par défaut.

Étape 2 Accédez au mode d'exécution privilégié.

enable

Lors de votre première saisie de la commande **enable**, vous devrez modifier le mot de passe.

Exemple :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

Le mot de passe d'activation que vous définissez sur l'ASA est également le mot de passe de l'utilisateur **administrateur** FXOS si l'ASA ne parvient pas à démarrer et que vous passez en mode Failsafe (sécurité intégrée) dans FXOS.

Toutes les commandes non liées à la configuration sont disponibles en mode d'exécution privilégié. Vous pouvez également passer en mode de configuration à partir du mode d'exécution privilégié.

Pour quitter le mode d'exécution privilégié, entrez la commande **disable**, **exit** ou **quit**.

Étape 3 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Vous pouvez commencer à configurer l'ASA à partir du mode de configuration globale. Pour quitter le mode de configuration globale, entrez la commande **exit**, **quit** ou **end**.

Étape 4 (Facultatif) Connectez-vous à l'Interface de ligne de commande FXOS.

connect fxos [**admin**]

- **admin** : fournit un accès au niveau administrateur. Sans cette option, les utilisateurs ont un accès en lecture seule. Notez qu'aucune commande de configuration n'est disponible même en mode admin.

Vous n'êtes pas invité à saisir les informations d'authentification de l'utilisateur. Le nom d'utilisateur actuel de l'ASA est transmis au moyen de FXOS, et aucune connexion supplémentaire n'est requise. Pour revenir à l'interface de ligne de commande de l'ASA, entrez **exit** ou tapez **Ctrl-Shift-6**, **x**.

À l'intérieur de FXOS, vous pouvez visualiser l'activité des utilisateurs en utilisant la commande **scope security/show audit-logs**.

Exemple :

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Accéder à la console ASA sur le Châssis Firepower 4100/9300

Pour la configuration initiale, accédez à l'interface de commande en ligne en vous connectant au superviseur Châssis Firepower 4100/9300 (au port de console ou à distance à l'aide de Telnet ou de SSH), puis en vous connectant au module de sécurité ASA.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande (console ou SSH) du superviseur Châssis Firepower 4100/9300 , puis connectez-vous à l'ASA :

connect module *slot* {**console** | **telnet**}

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

La première fois que vous accédez au module, vous accédez à l'interface de ligne de commande du module FXOS. Vous devez ensuite vous connecter à l'application ASA.

connect asa

Exemple :

```
Firepower# connect module 1 console
Firepower-module1> connect asa

asa>
```

Étape 2 Accédez au mode d'exécution privilégié, qui est le niveau de privilège le plus élevé.

enable

Lors de votre première saisie de la commande **enable**, vous devrez modifier le mot de passe.

Exemple :

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa#
```

Toutes les commandes non liées à la configuration sont disponibles en mode d'exécution privilégié. Vous pouvez également passer en mode de configuration à partir du mode d'exécution privilégié.

Pour quitter le mode privilégié, entrez la commande **disable**, **exit** ou **quit** .

Étape 3 Entrer en mode de configuration globale.

configure terminal

Exemple :

```
asa# configure terminal
asa(config)#
```

Pour quitter le mode de configuration globale, entrez la commande **disable**, **exit** ou **quit**.

Étape 4 Quittez la console d'application pour l'interface de ligne de commande du module FXOS en saisissant **Ctrl-a, d**

Vous souhaiterez peut-être utiliser l'interface de ligne de commande du module FXOS à des fins de résolution de problèmes.

Étape 5 Revenez au niveau de superviseur de l'Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

Activer le mode FIPS

La norme FIPS, ou Federal Information Processing Standard, est une norme de certification des États-Unis et du Canada. Elle définit les exigences que les modules cryptographiques doivent respecter. Certaines versions d'ASA sont conformes à la norme FIPS 140-3, conformément aux normes du National Institute of Standards (NIST) des États-Unis.

En plus d'activer FIPS sur l'ASA, vous devez également configurer des algorithmes de chiffrement conformes à FIPS.

Vous ne pouvez pas activer FIPS pour la mise en grappe.

Avant de commencer

- Le mode FIPS est uniquement pris en charge sur les versions qui ont fait l'objet de la conformité FIPS. Vous devez désactiver le mode FIPS avant d'effectuer la mise à niveau vers une version de conformité non FIPS.

  Pour savoir quelles versions sont conformes à la norme FIPS et pour afficher leurs certifications, consultez https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html?flt0_general-table0=asa.

- Pour le basculement, les deux unités doivent être en mode FIPS.

Procédure

Étape 1 Activez FIPS sur l'ASA.

fips enable

Exemple :

```
ciscoasa(config)# fips enable
WARNING: FIPS mode change will not take effect until you save configuration and reboot the
 device
```

Lorsque FIPS est activé, FIPS POST s'exécute et imprime le message de console suivant au démarrage :

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9
```

```
INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
ciscoasa>
```

Étape 2 Enregistrez la configuration et rechargez.

write memory

reload

Étape 3 (Facultatif) Exécutez les autotests de mise sous tension.

fips self-test poweron

Les tests comprennent le test d'algorithme cryptographique, le test d'intégrité logicielle et le test des fonctions critiques.

Configurer l'accès ASDM

Cette section décrit comment accéder à ASDM avec une configuration par défaut et comment configurer l'accès si vous n'avez pas de configuration par défaut.

Utiliser la configuration d'usine par défaut pour l'accès ASDM

Avec une configuration d'usine par défaut, la connectivité ASDM est préconfigurée avec les paramètres réseau par défaut.

Procédure

Connectez-vous à ASDM en utilisant les paramètres d'interface et de réseau suivants :

- L'interface de gestion dépend de votre modèle :
  - Firepower 1010 : Management 1/1 (192.168.45.1), ou Ethernet interne 1/2 à 1/8 (192.168.1.1). Les hôtes de gestion sont limités au réseau 192.168.45.0/24 et les hôtes internes sont limités au réseau 192.168.4.0/24.
  - Firepower 1100, 2100 en mode appareil, Secure Firewall 3100 : Ethernet interne 1/2 (192.168.1.1) ou Management 1/1 (à partir de DHCP). Les hôtes internes sont limités au réseau 192.168.1.0/24. Les hôtes de gestion sont autorisés dans tous les réseaux.
  - Firepower 2100 en mode plateforme : Management 1/1 (192.168.45.1). Les hôtes de gestion sont limités au réseau 192.168.45.0/24.
  - Firepower 4100/9300 : l'interface de type de gestion et l'adresse IP de votre choix définies lors du déploiement. Les hôtes de gestion sont autorisés dans tous les réseaux.
  - ASA virtuel : Management 0/0 (défini pendant le déploiement). Les hôtes de gestion sont limités au réseau de gestion.

- ISA 3000 : Management 1/1 (192.168.1.1). Les hôtes de gestion sont limités au réseau 192.168.1.0/24.

Remarque Si vous passez en mode de contexte multiple, vous pouvez accéder à ASDM à partir du contexte d'administration en utilisant les paramètres réseau ci-dessus.

Sujets connexes

Configurations d'usine par défaut, à la page 32
Activer ou désactiver le mode de contexte multiple, à la page 270
Démarrer ASDM, à la page 28

Personnaliser l'accès ASDM

Utilisation cette procédure si *une ou plusieurs* des conditions suivantes s'appliquent :

- Vous n'avez pas de configuration d'usine par défaut
- Vous souhaitez passer en mode de pare-feu transparent
- Vous souhaitez passer en mode de contexte multiple

Pour le mode routé et unique, pour un accès ASDM rapide et facile, nous vous conseillons d'appliquer la configuration d'usine par défaut avec la possibilité de définir votre propre adresse IP de gestion. Utilisez la procédure de cette section uniquement si vous avez des besoins particuliers, tels que la configuration du mode transparent ou de contexte multiple, ou si vous avez une autre configuration que vous devez conserver.

Remarque Pour l'ASAv, vous pouvez configurer le mode transparent lorsque vous le déployez; cette procédure est donc principalement utile après le déploiement si vous devez effacer votre configuration, par exemple.

Procédure

Étape 1 Accédez à l'interface de ligne de commande au niveau du port de console.

Étape 2 (Facultatif) Activez le mode de pare-feu transparent :

Cette commande efface votre configuration.

firewall transparent

Étape 3 Configurez l'interface de gestion :

```
interface interface_id
   nameif name
   security-level level
   no shutdown
```

ip address *ip_address mask*

Exemple :

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

Le **niveau de sécurité** est un nombre compris entre 1 et 100, où 100 désigne le niveau le plus sécurisé.

Étape 4 (Pour les hôtes de gestion directement connectés) Définissez le pool DHCP pour le réseau de gestion :

dhcpd address *ip_address-ip_address interface_name*
dhcpd enable *interface_name*

Exemple :

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

Assurez-vous de ne pas inclure l'adresse de l'interface dans la plage.

Étape 5 (Pour les hôtes de gestion à distance) Configurez une route vers les hôtes de gestion :

route *management_ifc management_host_ip mask gateway_ip* **1**

Exemple :

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

Étape 6 Activez le serveur HTTP pour ASDM :

http server enable

Étape 7 Autoriser le ou les hôte(s) de gestion à accéder à ASDM :

http *ip_address mask interface_name*

Exemple :

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

Étape 8 Enregistrez la configuration :

write memory

Étape 9 (Facultatif) Définissez le mode sur plusieurs modes :

mode multiple

Lorsque vous y êtes invité, confirmez que vous souhaitez convertir la configuration existante pour en faire le contexte d'administration. Vous êtes alors invité à recharger l'ASA.

Exemples

La configuration suivante convertit le mode de pare-feu en mode transparent, configure l'interface de gestion Management 0/0 et active ASDM pour un hôte de gestion :

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

Sujets connexes

Rétablir les valeurs par défaut de la configuration, à la page 33
Définir le mode du pare-feu (mode unique), à la page 231
Accéder à la console de l'ISA 3000, à la page 17
Démarrer ASDM, à la page 28

Démarrer ASDM

Lancez ASDM à l'aide du lanceur ASDM. Le lanceur est une application téléchargée à partir de l'ASA à l'aide d'un navigateur que vous pouvez utiliser pour vous connecter à n'importe quelle adresse IP ASA. Vous n'avez pas besoin de télécharger à nouveau le lanceur si vous souhaitez vous connecter à d'autres ASA.

Dans ASDM, vous pouvez choisir une autre adresse IP ASA à gérer.

Cette section décrit comment se connecter à ASDM pour la première fois, puis lancer ASDM à l'aide du lanceur.

ASDM stocke les fichiers dans le répertoire \Users\<user_id>\.asdm, y compris le cache, le journal et les préférences, ainsi que dans le répertoire Temp, y compris les profils Secure Client (services client sécurisés).

Procédure

Étape 1 Sur le PC que vous avez spécifié comme client ASDM, saisissez l'URL suivante :

https://*asa_ip_address*/**admin**

Remarque Assurez-vous de préciser **https://** et **http://** ou simplement l'adresse IP (par défaut HTTP); l'ASA ne transfère pas automatiquement une requête HTTP vers HTTPS.

La page de lancement ASDM apparaît avec les boutons suivants :

Installer le lanceur ASDM

Étape 2 Pour télécharger le lanceur et démarrer ASDM :

a) Cliquez sur **Install ASDM Launcher**.

Illustration 2 : Installer le lanceur ASDM



b) Laissez les champs du nom d'utilisateur et du mot de passe vides (pour une nouvelle installation), puis cliquez sur **OK**.

En l'absence d'authentification HTTPS, vous pouvez accéder à ASDM sans nom d'utilisateur et mot de passe **d'activation**, qui est vide par défaut. Lorsque vous saisissez la commande **enable** au niveau de l'interface de ligne de commande pour la première fois, vous êtes invité à modifier le mot de passe; ce comportement n'est pas appliqué lorsque vous vous connectez à ASDM. Nous vous suggérons de modifier le mot de passe d'activation dès que possible afin qu'il ne reste pas vide; voir Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet, à la page 759. **Remarque** : Si vous avez activé l'authentification HTTPS, saisissez votre nom d'utilisateur et le mot de passe associé. Même sans authentification, si vous saisissez un nom d'utilisateur et un mot de passe à l'écran de connexion (au lieu de laisser le nom d'utilisateur vide), ASDM vérifie la base de données locale à la recherche d'une correspondance.

c) Enregistrez le programme d'installation sur votre ordinateur, puis démarrez le programme d'installation. Le lanceur ASDM s'ouvre automatiquement une fois l'installation terminée.

d) Saisissez la gestion des adresses IP, le même nom d'utilisateur et mot de passe (vide pour une nouvelle installation), puis cliquez sur **OK**.

Personnaliser le fonctionnement ASDM

Vous pouvez installer un certificat d'identité pour lancer ASDM avec succès et augmenter la mémoire du paquet ASDM afin qu'il puisse gérer des configurations plus importantes.

Installer un certificat d'identité pour ASDM

Lorsque vous utilisez la mise à jour 51 de Java 7 et les versions ultérieures, le lanceur ASDM nécessite un certificat de confiance. Une méthode simple pour répondre aux exigences en matière de certificats consiste à installer un certificat d'identité autosigné.

Consultez le document suivant pour installer un certificat d'identité autosigné sur l'ASA afin de l'utiliser avec ASDM, et pour enregistrer le certificat avec Java.

http://www.cisco.com/go/asdm-certificate

Augmenter la mémoire de configuration de l'ASDM

ASDM prend en charge une taille de configuration maximale de 512 Ko. Si vous dépassez cette quantité, vous risquez de rencontrer des problèmes de performance. Par exemple, lorsque vous chargez la configuration, la boîte de dialogue d'état indique le pourcentage de la configuration qui est terminée, mais avec des configurations importantes, elle cesse de s'augmenter et semble suspendre l'opération, même si ASDM est toujours en train de traiter la configuration. Si cette situation se produit, nous vous recommandons d'augmenter la mémoire vive du système ASDM. Pour confirmer que vous subissez un épuisement de la mémoire, supervisez la console Java pour détecter le message « java.lang.OutOfMemoryError ».

En outre, nous vous conseillons de réduire la taille de votre configuration si possible, par exemple en supprimant les objets inutilisés.

Augmenter la mémoire de configuration de l'ASDM sous Windows

Pour augmenter la taille de la mémoire du tas ASDM, modifiez le fichier **run.bat** en suivant la procédure suivante.

Procédure

Étape 1 Aller dans le répertoire d'installation d'ASDM, par exemple C :\NProgram Files (x86)\NCisco Systems\NASDM.

Étape 2 Modifiez le fichier **run.bat** à l'aide d'un éditeur de texte.

Étape 3 Dans la ligne qui commence par « start javaw.exe », modifiez l'argument préfixé par « -Xmx » pour préciser la taille du tas souhaitée. Par exemple, remplacez-la par -Xmx768M pour 768 Mo ou -Xmx1G pour 1 Go.

Pour les configurations très volumineuses, vous devrez peut-être spécifier une taille de pile allant jusqu'à 2 Go.

Étape 4 Enregistrez le fichier **run.bat** .

Augmenter la mémoire de configuration de l'ASDM sous Mac OS

Pour augmenter la taille de la mémoire du tas ASDM, modifiez le fichier **Info.plist** en suivant la procédure suivante.

Procédure

Étape 1 Cliquez avec le bouton droit de la souris sur l'icône **Cisco ASDM-IDM** et choisissez **Show Package Contents** (afficher le contenu du paquet).

Étape 2 Dans le dossier **Contents** (contenus), double-cliquez sur le fichier **Info.plist**. Si les outils de développeur sont installés, ils s'ouvrent dans le **Property List Editor** (Éditeur de liste de propriétés). Sinon, ils s'ouvrent dans **TextEdit**.

Étape 3 Sous **Java** > **VMOptions**, modifiez la chaîne préfixée par « -Xmx » pour préciser la taille du tas souhaitée. Par exemple, remplacez-la par -Xmx768M pour 768 Mo ou -Xmx1G pour 1 Go.

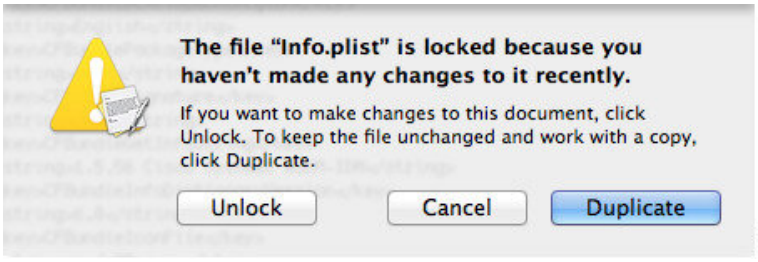
```
    <key>CFBundleIconFile</key>
    <string>asdm32.icns</string>

    <key>VMOptions</key>
    <string>-Xms64m -Xmx512m</string>


  <key>CFBundleDocumentTypes</key>
    <array>
```

Pour les configurations très volumineuses, vous devrez peut-être spécifier une taille de pile allant jusqu'à 2 Go.

Étape 4 Si ce fichier est verrouillé, une erreur telle que la suivante s'affiche :



Étape 5 Cliquez sur **Unlock** (déverrouiller) et enregistrez le fichier.

Si vous ne voyez pas la boîte de dialogue **Unlock** (déverrouiller), quittez l'éditeur, cliquez avec le bouton droit de la souris sur l'icône **Cisco ASDM-IDM**, choisissez **Copy Cisco ASDM-IDM** (copier Cisco ASDM-IDM), et collez-le à un endroit où vous avez des droits d'écriture, comme le bureau. Modifiez ensuite la taille du tas à partir de cette copie.

Configurations d'usine par défaut

La configuration d'usine par défaut est la configuration appliquée par Cisco aux nouveaux ASA.

- Firepower 1010 : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion ou des ports de commutation internes.
- Firepower 1100 : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion ou de l'interface interne.
- Firepower 2100 —Mode plateforme (par défaut) : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide de Secure Firewall Chassis Manager (anciennement Firepower Chassis Manager) et d'ASDM à partir de l'interface de gestion.

  Mode appareil : si vous passez en mode appareil, la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion ou de l'interface interne.
- Secure Firewall 3100 : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion Management 1/1 ou de l'interface interne.
- Châssis Firepower 4100/9300 : lorsque vous déployez l'unité autonome ou une grappe d'ASA, la configuration d'usine par défaut configure une interface pour la gestion afin que vous puissiez vous y connecter à l'aide d'ASDM, avec lequel vous pouvez ensuite terminer votre configuration.
- ASA virtuel : en fonction de votre hyperviseur, dans le cadre du déploiement, la configuration de déploiement (les paramètres de déploiement virtuel initiaux) configure une interface pour la gestion afin que vous puissiez vous y connecter à l'aide d'ASDM, avec lequel vous pouvez ensuite terminer votre configuration. Vous pouvez également configurer des adresses IP de basculement. Vous pouvez également appliquer une configuration « d'usine par défaut » si vous le souhaitez.
- ISA 3000 : la configuration par défaut est une configuration en mode de pare-feu transparent presque complète avec toutes les interfaces internes et externes sur le même réseau; vous pouvez vous connecter à l'interface de gestion avec ASDM pour définir l'adresse IP de votre réseau. Le contournement matériel est activé pour deux paires d'interfaces .

Pour les appareils, la configuration d'usine par défaut est disponible uniquement pour le mode de pare-feu routé et le mode de contexte unique, sauf pour l'ISA 3000, où la configuration d'usine par défaut n'est disponible qu'en mode transparent. Pour l'ASA virtuel et leChâssis Firepower 4100/9300 , vous pouvez choisir le mode transparent ou routé lors du déploiement.



Remarque En plus des fichiers image et de la configuration (masquée) par défaut, les dossiers et fichiers suivants sont standard dans la mémoire flash : log/, crypto_archive/ et coredumpinfo/coredump.cfg. La date de ces fichiers peut ne pas correspondre à celle des fichiers image dans la mémoire flash. Ces fichiers facilitent le dépannage potentiel; ils n'indiquent pas qu'une défaillance s'est produite.

Rétablir les valeurs par défaut de la configuration

Cette section décrit comment restaurer les valeurs par défaut de la configuration. Les procédures de l'interface de ligne de commande et ASDM sont fournies. Pour l'ASA virtuel, cette procédure efface la configuration de déploiement et applique la configuration suivante :

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
!
asdm logging informational
asdm history enable
!
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```



Remarque Sur le Firepower 4100/9300, la restauration de la configuration d'usine par défaut efface simplement la configuration; pour restaurer la configuration par défaut, vous devez redéployer l'ASA à partir du superviseur.

Avant de commencer

Cette fonctionnalité est disponible uniquement en mode de pare-feu routé, sauf pour l'ISA 3000, où cette commande est prise en charge uniquement en mode transparent. En outre, cette fonctionnalité est disponible uniquement en mode de contexte unique; un ASA avec une configuration effacée n'a pas de contextes définis à configurer automatiquement à l'aide de cette fonctionnalité.

Procédure

Étape 1 Restaurez les valeurs par défaut de la configuration :

configure factory-default [*ip_address* [*mask*]]

Exemple :

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```



Remarque Cette commande ne supprime pas le mode (appareil ou plateforme) actuellement défini pour Firepower 2100.

Si vous spécifiez l'*ip_address*, vous définissez l'adresse IP interne ou de l'interface de gestion, selon votre modèle, au lieu d'utiliser l'adresse IP par défaut. Consultez les directives de modèle suivantes pour savoir quelle interface est définie par l'option *ip_address* :

- Firepower 1010 : définit l'adresse IP de l'interface de **gestion**.
- Firepower 1100 : définit l'adresse IP de l'interface **interne**.
- Firepower 2100 en mode appareil : définit l'adresse IP de l'interface **interne**.
- Firepower 2100 en mode plateforme : définit l'adresse IP de l'interface de **gestion**.
- Secure Firewall 3100 : définit l'adresse IP de l'interface **interne**.
- Firepower 4100/9300 : aucun effet.
- ASA virtuel : définit l'adresse IP de l'interface de **gestion**.
- ISA 3000 : définit l'adresse IP de l'interface de **gestion**.

La commande **http** utilise le sous-réseau que vous spécifiez. De même, la plage de commandes **dhcpd address** se compose de toutes les adresses disponibles supérieures à l'adresse IP que vous spécifiez. Par exemple, si vous spécifiez 10.5.6.78 avec un filtre d'adresse locale 255.255.255.0, la plage d'adresses DHCP sera 10.5.6.79-10.5.6.254.

Pour Firepower 1000 et Firepower 2100 en mode appareil, et Secure Firewall 3100, 6100 : cette commande efface la **boot system**commande, si elle est présente, ainsi que le reste de la configuration. Cette modification de configuration n'affecte pas l'image au démarrage : l'image actuellement chargée continue d'être utilisée.

Pour Firepower 2100 en mode plateforme : ce modèle n'utilise pas la commande **boot system**; les paquets sont gérés par FXOS.

Pour tous les autres modèles : cette commande efface la commande **boot system**, si elle est présente, ainsi que le reste de la configuration. La commande **boot system** vous permet de démarrer à partir d'une image en particulier. La prochaine fois que vous rechargez l'ASA après avoir restauré la configuration d'usine, il démarre à partir de la première image de la mémoire flash interne; si vous n'avez pas d'image dans la mémoire flash interne, l'ASA ne démarre pas.

Exemple :

```
docs-bxb-asa3(config)# configure factory-default 10.86.203.151 255.255.254.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
WARNING: The new maximum-session limit will take effect after the running-config is saved
and the system boots next time. Command accepted
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.86.203.151 255.255.254.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.86.202.0 255.255.254.0 management
Executing command: dhcpd address 10.86.203.152-10.86.203.254 management
```

```
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Étape 2 Enregistrez la configuration par défaut dans la mémoire flash :

write memory

Cette commande enregistre la configuration d'exécution à l'emplacement par défaut pour la configuration de démarrage, même si vous avez précédemment configuré la commande **boot** pour définir un emplacement différent; lorsque la configuration a été effacée, ce chemin a également été effacé.

Étape 3 (Procédure ASDM.) Dans la fenêtre d'application principale d'ASDM, procédez comme suit :

a) Choisissez **File (Fichier)** > **Reset Device to the Factory Default Configuration (Réinitialiser le périphérique à la configuration d'usine par défaut)**.

La boîte de dialogue **Reset Device to the Default Configuration (Réinitialiser le périphérique à la configuration par défaut)** apparaît.

b) (Facultatif) Renseignez le champ **Management IP address** (Adresse IP de gestion) de l'interface de gestion ou interne, au lieu d'utiliser l'adresse par défaut.

Consultez l'étape précédente relative à l'interface de ligne de commande pour en savoir plus sur l'adresse IP d'interface définie par modèle.

c) (Facultatif) Choisissez le **Management Subnet Mask** (Filtre d'adresse locale de gestion) dans la liste déroulante.

d) Cliquez sur **OK**.

Une boîte de dialogue de confirmation s'affiche.

Remarque Pour Firepower 1000 et Firepower 2100 en mode appareil, et Secure Firewall 3100 : cette commande efface l'emplacement de l'image de démarrage, si elle est présente, ainsi que le reste de la configuration. Cette modification de configuration n'affecte pas l'image au démarrage : l'image actuellement chargée continue d'être utilisée.

Pour Firepower 2100 en mode plateforme : ce modèle n'utilise pas l'emplacement de l'image de démarrage; les paquets sont gérés par FXOS.

Pour tous les autres modèles : cette action efface également l'emplacement de l'image de démarrage, si elle est présente, ainsi que le reste de la configuration. Le volet **Configuration > Device Management (Gestion des périphériques) > System Image/Configuration (Configuration système/image) > Boot Image/Configuration (Image de démarrage/Configuration)** vous permet de démarrer à partir d'une image en particulier, y compris une image sur la mémoire externe. La prochaine fois que vous rechargez l'ASA après avoir restauré la configuration d'usine, il démarre à partir de la première image de la mémoire flash interne; si vous n'avez pas d'image dans la mémoire flash *interne*, l'ASA ne démarre pas.

e) Cliquez sur **Oui**.

f) Après avoir restauré la configuration par défaut, enregistrez cette configuration dans la mémoire flash interne. Choisissez **File (Fichier)** > **Save Running Configuration to Flash (Enregistrer la configuration en cours d'exécution dans la mémoire flash)**.

Le choix de cette option enregistre la configuration d'exécution à l'emplacement par défaut pour la configuration de démarrage, même si vous avez déjà configuré un emplacement différent. Lorsque la configuration a été effacée, ce chemin a également été effacé.

Restaurer la configuration du déploiement de l'ASA virtuel

Cette section décrit comment restaurer la configuration du déploiement de l'ASA virtuel (Day0).

Procédure

Étape 1 Pour le basculement, mettez hors tension l'unité en veille.

Pour empêcher l'unité en veille de devenir active, vous devez l'éteindre. Si vous la laissez activée, lorsque vous effacez la configuration de l'unité active, l'unité en veille devient active. Lorsque l'ancienne unité active se recharge et se reconnecte via la liaison de basculement, l'ancienne configuration sera synchronisée à partir de la nouvelle unité active, effaçant ainsi la configuration de déploiement souhaitée.

Étape 2 Restaurez la configuration de déploiement après le rechargement. Pour le basculement, saisissez cette commande sur l'unité active :

write erase

Remarque L'ASA virtuel démarre l'image en cours d'exécution, de sorte que vous n'êtes pas revenu à l'image de démarrage d'origine. Pour utiliser l'image de démarrage d'origine, consultez la commande **boot image**.

N'enregistrez pas la configuration.

Étape 3 Rechargez l'ASA virtuel et chargez la configuration de déploiement :

reload

Étape 4 Pour le basculement, mettez sous tension l'unité en veille.

Après le rechargement de l'unité active, mettez sous tension l'unité en veille. La configuration de déploiement se synchronisera avec l'unité en veille.

Configuration par défaut de Firepower 1010

La configuration d'usine par défaut du Firepower 1010 concerne les éléments suivants :

- **Commutateur matériel** : Ethernet 1/2 à 1/8 appartient à VLAN 1
- **inside→outside (flux de trafic)** : Ethernet 1/1 (externe), VLAN1 (interne)
- **management** (gestion) : Management 1/1 (gestion), adresse IP 192.168.45.1

- **adresse IP externe** de DHCP, **adresse IP interne** — 192.168.1.1
- **serveur DHCP** sur interface interne, interface de gestion
- **Voie de routage par défaut** depuis l'extérieur de DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes de gestion sont limités au réseau 192.168.45.0/24 et les hôtes internes sont limités au réseau 192.168.4.0/24.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
```

```
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Configuration par défaut de Firepower 1100

La configuration d'usine par défaut du Firepower 1100 concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, **adresse IP interne**—192.168.1.1
- **gestion**—Management 1/1 (gestion), adresse IP de DHCP
- **serveur DHCP** sur interface interne
- **Routes par défaut** depuis l'extérieur de DHCP, gestion DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes internes sont limités au réseau 192.168.1.0/24.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
```

```
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Configuration par défaut du mode plateforme de Firepower 2100

Vous pouvez configurer Firepower 2100 pour un fonctionnement en mode plateforme; le mode appareil est le mode par défaut.

Remarque Pour les versions antérieures à la version 9.13 (1), le mode plateforme était la seule option par défaut. Si vous effectuez une mise à niveau à partir du mode plateforme, ce mode est maintenu.

Configuration ASA

La configuration d'usine par défaut d'ASA sur Firepower 2100 concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, adresse IP interne — 192.168.1.1
- **serveur DHCP** sur interface interne
- **Voie de routage par défaut** depuis l'extérieur de DHCP
- **management** (gestion) : Management 1/1 (gestion), adresse IP 192.168.45.1
- Accès **ASDM** : hôtes de gestion.

- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Initialisation du trafic de **gestion FXOS** : le châssis FXOS peut initier le trafic de gestion sur l'interface externe ASA.
- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address 192.168.45.1 255.255.255.0
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.45.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
ip-client outside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
```

Configuration FXOS

La configuration d'usine par défaut de FXOS sur Firepower 2100 concerne les éléments suivants :

- **Interface Management 1/1** : adresse IP 192.168.45.45
- **Passerelle par défaut** : interfaces de données ASA
- **Firewall Chassis Manager et l'accès SSH** : depuis le réseau du gestionnaire uniquement.
- **Nom d'utilisateur par défaut** : le nom d'utilisateur **admin** et le mot de passe par défaut **Admin123**.
- **Serveur DHCP** : plage d'adresses IP de clients 192.168.45.10-192.168.45.12

- **NTP** : Serveurs NTP de Cisco : 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org
- Serveurs **DNS** , OpenDNS : 208.67.222.222, 208.67.220.220
- **Ethernet 1/1 et Ethernet 1/2** : activés

Configuration par défaut du mode appareil de Firepower 2100

Le Firepower 2100 fonctionne en mode Appliance (appareil) par défaut.



Remarque Pour les versions antérieures à la version 9.13 (1), le mode plateforme était la seule option par défaut. Si vous effectuez une mise à niveau à partir du mode plateforme, le mode plateforme est maintenu.

La configuration d'usine par défaut pour le Firepower 2100 en mode appareil concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, **adresse IP interne**—192.168.1.1
- **adresse IP de gestion** : depuis DHCP—Management 1/1 (gestion)
- **serveur DHCP** sur interface interne
- **Routes par défaut** depuis l'extérieur de DHCP, gestion DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes internes sont limités au réseau 192.168.1.0/24.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
```

```
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Configuration par défaut de Secure Firewall 3100

La configuration d'usine par défaut pour Secure Firewall 3100 concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, **adresse IP interne**—192.168.1.1
- **gestion**—Management 1/1 (gestion), adresse IP de DHCP
- **serveur DHCP** sur interface interne
- **Routes par défaut** depuis l'extérieur de DHCP, gestion DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes internes sont limités au réseau 192.168.1.0/24.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
```

```
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Configuration par défaut de Châssis Firepower 4100/9300

Lorsque vous déployez l'ASA sur le Châssis Firepower 4100/9300 , vous pouvez prédéfinir de nombreux paramètres qui vous permettent de vous connecter à l'interface de gestion à l'aide d'ASDM. Une configuration typique comprend les paramètres suivants :

- Interface de gestion :
  - Interface de type de gestion de votre choix définie sur le superviseur Châssis Firepower 4100/9300
  - Nommée « gestion »
  - Adresse IP de votre choix
  - Niveau de sécurité 0
  - Gestion uniquement
- Route par défaut via l'interface de gestion
- Accès ASDM : tous les hôtes autorisés.

La configuration d'une unité autonome comprend les commandes suivantes. Pour une configuration supplémentaire des unités en grappe, consultez Créer une grappe ASA, à la page 468.

```
interface <management_ifc>
  management-only
  ip address <ip_address> <mask>
  ipv6 address <ipv6_address>
  ipv6 enable
  nameif management
  security-level 0
  no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

Configuration par défaut d'ISA 3000

La configuration d'usine par défaut pour ISA 3000 concerne les éléments suivants :

- **Transparent firewall mode** (Mode de pare-feu transparent) : un pare-feu transparent est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.
- **1 Bridge Virtual Interface** (1 interface virtuelle de pont) : toutes les interfaces membres se trouvent dans le même réseau (**adresse IP *non* préconfigurée; vous devez le définir pour qu'il corresponde à votre réseau**) : GigabitEthernet 1/1 (outside1), GigabitEthernet 1/2 (inside1), GigabitEthernet 1/3 (inside2), GigabitEthernet 1/4 (inside2)
- Toutes les interfaces **internes et externes** peuvent communiquer entre elles.
- Interface **Management 1/1** : 192.168.1.1/24 pour l'accès à ASDM.
- **DHCP** pour les clients sur la gestion.
- Accès **ASDM** : hôtes de gestion.
- L'option **Hardware bypass** (Contournement matériel) est activée pour les paires d'interfaces suivantes : GigabitEthernet 1/1 et 1/2; GigabitEthernet 1/3 et 1/4



Remarque Lorsque l'ISA 3000 perd de l'alimentation et passe en mode de contournement matériel, seules les paires d'interfaces ci-dessus peuvent communiquer; inside1 et inside2, et outside1 et outside2 ne peuvent plus communiquer. Toutes les connexions existantes entre ces interfaces seront perdues. Lorsque l'alimentation revient, il y a une brève interruption de la connexion lorsque l'ASA prend en charge les flux.

La configuration comprend les commandes suivantes :

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
```

```
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management
```

Configuration du déploiement ASA virtuel

Lorsque vous déployez l'ASA virtuel, vous pouvez prédéfinir de nombreux paramètres qui vous permettent de vous connecter à l'interface de gestion Management 0/0 à l'aide d'ASDM. Une configuration typique comprend les paramètres suivants :

- Mode de pare-feu routé ou transparent
- Interface de gestion Management 0/0 :
  - Nommée « gestion »
  - Adresse IP ou DHCP
  - Niveau de sécurité 0
- Route statique pour l'adresse IP de l'hôte de gestion (s'il ne se trouve pas sur le sous-réseau de gestion)
- Serveur HTTP activé ou désactivé
- Accès HTTP pour l'adresse IP de l'hôte de gestion
- (Facultatif) Adresses IP de liaison de basculement pour GigabitEthernet 0/8 et adresse IP de secours Management 0/0
- Serveur DNS
- Jeton d'ID de licence Smart
- Niveau de débit de la licence Smart et niveau de fonctionnalité Essentials
- (Facultatif) URL et port du mandataire HTTP Smart Call Home
- (Facultatif) Paramètres de gestion SSH :

- Adresses IP du client
- Nom d'utilisateur et mot de passe locaux
- Authentification requise pour SSH à l'aide de la base de données LOCALE

- (Facultatif) API REST activée ou désactivée

Remarque Pour enregistrer avec succès l'ASA virtuel auprès de l'autorité de licence de Cisco, l'ASA virtuel nécessite un accès Internet. Vous devrez peut-être effectuer une configuration supplémentaire après le déploiement pour obtenir un accès Internet et un enregistrement de licence réussi.

Consultez l'exemple de configuration suivant pour une unité autonome :

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
http server enable
http managemment_host_IP mask management
route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
```

Remarque La licence Essentials était appelée licence « Standard ».

Consultez l'exemple de configuration suivant pour une unité principale dans une paire de basculement :

```
nameif management
  security-level 0
  ip address ip_address standby standby_ip

  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
```

```
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

Régler le Firepower 2100 en mode appareil ou plateforme

Le Firepower 2100 exécute un système d'exploitation sous-jacent appelé le FXOS. Vous pouvez exécuter Firepower 2100 dans les modes suivants :

- Mode appareil (par défaut) : le mode appareil vous permet de configurer tous les paramètres de l'ASA. Seules les commandes de dépannage avancées sont disponibles à partir de l'interface de ligne de commande de FXOS.
- Mode plateforme : lorsque vous êtes en mode plateforme (Platform), vous devez configurer les paramètres de fonctionnement de base et les paramètres de l'interface matérielle dans FXOS. Ces paramètres comprennent l'activation des interfaces, l'établissement de canaux EtherChannels, du protocole NTP, de la gestion des images, etc. Vous pouvez utiliser l'interface web Firewall Chassis Manager ou l'interface de ligne de commande FXOS. Vous pouvez ensuite configurer votre politique de sécurité dans le système d'exploitation ASA en utilisant ASDM ou l'interface de ligne de commande de l'ASA.

Cette procédure vous explique comment changer de mode.

Mise en garde Lorsque vous modifiez le mode, vous devez recharger le système, et la configuration est effacée. La configuration par défaut est appliquée au rechargement. Assurez-vous de conserver une copie de la configuration d'origine pour référence.

Vous observez que les commandes **clear configure all** et **configure factory-default** ne suppriment pas le mode actuel.

Avant de commencer

Vous ne pouvez changer de mode qu'au niveau de l'interface de ligne de commande.

Procédure

Étape 1 (Facultatif) Sauvegardez votre configuration actuelle. Consultez Sauvegarde et restauration de configurations ou d'autres fichiers, à la page 1203

Bien qu'il existe de légères différences entre une configuration en mode appareil et une configuration en mode plateforme, une copie de l'ancienne configuration peut constituer un bon point de départ. Par exemple, en mode plateforme, la configuration du protocole NTP, du système DNS et du canal EtherChannel ne fait pas partie de la configuration de l'ASA; elle ne sera donc pas incluse dans votre sauvegarde, mais la plupart des autres paramètres de l'ASA sont valides pour les deux modes.

Étape 2 Affichez le mode actuel.

show fxos mode

Exemple :

```
ciscoasa(config)# show fxos mode
Mode is currently set to appliance
```

Étape 3 Définissez le mode selon le mode plateforme.

no fxos mode appliance

write memory

reload

Après avoir défini le mode, vous devez enregistrer la configuration et recharger le périphérique. Avant le rechargement, vous pouvez rétablir la valeur d'origine du mode sans interruption.

Mise en garde Lorsque vous rechargez, la configuration est effacée. La configuration par défaut est appliquée au rechargement.

Exemple :

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

Étape 4 Définissez le mode selon le mode appareil.

fxos mode appliance

write memory

reload

Après avoir défini le mode, vous devez enregistrer la configuration et recharger le périphérique. Avant le rechargement, vous pouvez rétablir la valeur d'origine du mode sans interruption.

Mise en garde Lorsque vous rechargez, la configuration est effacée. La configuration par défaut est appliquée au rechargement.

Exemple :

```
ciscoasa(config)# fxos mode appliance
Mode set to appliance mode
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

Commencer avec la configuration

Pour configurer et superviser l'ASA, procédez comme suit.

Remarque ASDM prend en charge une configuration maximale de 512 Ko. Si vous dépassez cette limite, vous risquez de rencontrer des problèmes de performances. Consultez Augmenter la mémoire de configuration de l'ASDM, à la page 30.

Procédure

Étape 1 Pour la configuration initiale à l'aide de l'assistant de démarrage, choisissez **Wizards (Assistants)** > **Startup Wizard (Assistant de démarrage)**.

Étape 2 Pour utiliser l'assistant VPN IPsec pour configurer les connexions VPN IPsec, sélectionnez **Wizards (Assistants)** > **IPsec VPN Wizard (Assistant VPN IPsec)** et complétez chaque écran qui s'affiche.

Étape 3 Si vous souhaitez utiliser l'assistant SSL VPN pour configurer les connexions SSL VPN, sélectionnez **Wizards (Assistants)** > **SSL VPN Wizard (Assistant SSL VPN)** et complétez chaque écran qui s'affiche.

Étape 4 Pour configurer les paramètres de haute disponibilité et d'évolutivité, choisissez **Wizards (Assistants)** > **High Availability and Scalability Wizard (Assistant de haute disponibilité et d'évolutivité)**.

Étape 5 Si vous souhaitez utiliser l'assistant de capture de paquets pour configurer la capture de paquets, sélectionnez **Wizards (Assistants)** > **Packet Capture Wizard (Assistant de capture de paquets)**.

Étape 6 Pour afficher les différentes couleurs et les différents styles disponibles dans l'interface graphique utilisateur d'ASDM, choisissez **View (Afficher)** > **Office Look and Feel (Aspect et convivialité du bureau)**.

Étape 7 Pour configurer les fonctionnalités, cliquez sur le bouton **Configuration** dans la barre d'outils, puis cliquez sur l'un des boutons de fonctionnalité pour afficher le volet de configuration associé.

Remarque Si le champ Configuration est vide, cliquez sur **Refresh** (Actualiser) dans la barre d'outils pour afficher le contenu de l'écran.

Étape 8 Pour superviser l'ASA, cliquez sur le bouton **Monitoring** (Supervision) dans la barre d'outils, puis cliquez sur un bouton de fonctionnalité pour afficher le volet de supervision associé.

Utiliser l'outil d'interface de ligne de commande dans ASDM

Cette section explique comment saisir des commandes à l'aide d'ASDM et comment utiliser l'interface de ligne de commande.

Utiliser l'outil d'interface de ligne de commande

Cette fonctionnalité fournit un outil texte pour envoyer des commandes à l'ASA et afficher les résultats.

Les commandes que vous pouvez saisir avec l'outil d'interface de ligne de commande dépendent de vos privilèges d'utilisateur. Passez en revue votre niveau de privilège dans la barre d'état au bas de la fenêtre d'application principale d'ASDM pour vous assurer que vous disposez des privilèges requis pour exécuter les commandes d'interface de ligne de commande de niveau privilégié.

Avant de commencer

- Les commandes saisies dans l'outil d'interface de ligne de commande d'ASDM peuvent fonctionner différemment de celles saisies par le biais d'une connexion de terminal à l'ASA.
- Erreurs de commande : si une erreur se produit parce que vous avez saisi une commande incorrecte, la commande incorrecte est ignorée et les commandes restantes sont traitées. Un message s'affiche dans la zone Response (Réponse) pour vous informer si une erreur s'est produite ou non, ainsi que d'autres renseignements connexes.
- Commandes interactives : les commandes interactives ne sont pas prises en charge dans l'outil d'interface de ligne de commande. Pour utiliser ces commandes dans ASDM, utilisez le mot clé **noconfirm** s'il est disponible, comme indiqué dans la commande suivante :

```
crypto key generate rsa modulus 1024 noconfirm
```

- Évitez les conflits avec d'autres administrateurs : plusieurs utilisateurs administratifs peuvent mettre à jour la configuration en cours d'exécution de l'ASA. Avant d'utiliser l'outil d'interface de ligne de commande d'ASDM pour apporter des modifications à la configuration, vérifiez qu'il y a d'autres sessions administratives actives. Si plusieurs utilisateurs configurent l'ASA en même temps, les modifications les plus récentes prennent effet.

  Pour afficher d'autres sessions administratives qui sont actuellement actives sur le même ASA, choisissez **Monitoring (Supervision) > Propriétés (Propriétés) > Device Access (Accès au périphérique)**.

Procédure

Étape 1 Dans la fenêtre d'application principale d'ASDM, choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

La boîte de dialogue **Command Line Interface** (Interface de ligne de commande) apparaît.

Étape 2 Choisissez le type de commande (ligne unique ou plusieurs lignes) que vous souhaitez, puis choisissez la commande dans la liste déroulante ou saisissez-la dans le champ fourni.

Étape 3 Cliquez sur **Send** (Envoyer) pour exécuter la commande.

Étape 4 Pour saisir une nouvelle commande, cliquez sur **Clear Response** (Effacer la réponse), puis choisissez (ou saisissez) une autre commande à exécuter.

Étape 5 Cochez la case **Enable context-sensitive help (?)** (Activer l'aide contextuelle (?)) pour fournir une aide contextuelle pour cette fonctionnalité. Décochez cette case pour désactiver l'aide contextuelle.

Étape 6 Après avoir fermé la boîte de dialogue **Command Line Interface** (Interface de ligne de commande), si vous avez modifié la configuration, cliquez sur **Refresh** (Actualiser) pour afficher les modifications dans ASDM.

Afficher les commandes ignorées par ASDM sur l'appareil

Cette fonctionnalité vous permet d'afficher la liste des commandes non prises en charge par ASDM. En règle générale, ASDM les ignore. ASDM ne modifie ni ne supprime ces commandes de votre configuration en cours d'exécution. Consultez Commandes non prises en charge, à la page 90 pour de plus amples renseignements.

Procédure

Étape 1 Dans la fenêtre d'application principale d'ASDM, choisissez **Tools (Outils)** > **Show Commands Ignored by ASDM on Device (Afficher les commandes ignorées par ASDM sur le périphérique)**.

Étape 2 Cliquez sur **OK** lorsque vous avez terminé.

Appliquer les modifications de configuration aux connexions

Lorsque vous apportez des modifications à la configuration de la politique de sécurité, toutes les *nouvelles* connexions utilisent la nouvelle politique de sécurité. Les connexions existantes continuent d'utiliser la politique qui était configurée au moment de l'établissement de la connexion. La sortie de la commande **show** pour les anciennes connexions reflète l'ancienne configuration et, dans certains cas, n'inclura pas de données sur les anciennes connexions.

Par exemple, si vous supprimez une **politique de service** QoS d'une interface, puis ajoutez une version modifiée, la commande **show service-policy** affiche uniquement les compteurs QoS associés aux nouvelles connexions qui correspondent à la nouvelle politique de service; les connexions existantes sur l'ancienne politique ne s'affichent plus dans la sortie de la commande.

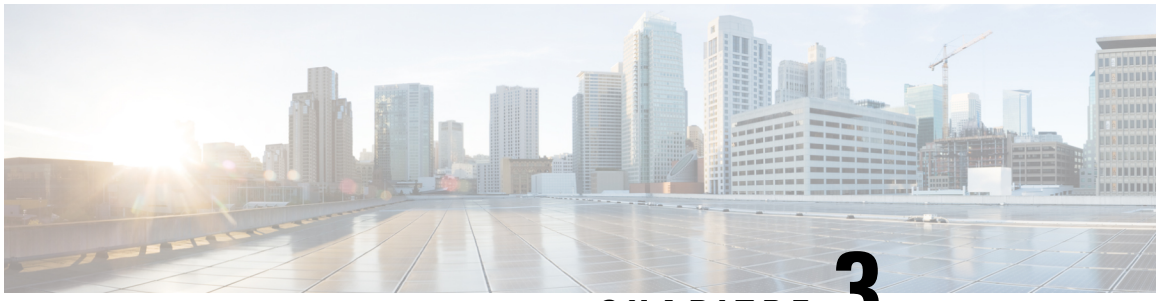
Pour vous assurer que toutes les connexions utilisent la nouvelle politique, vous devez déconnecter les connexions actuelles afin qu'elles puissent se reconnecter à l'aide de la nouvelle politique.

Pour déconnecter les connexions, saisissez la commande suivante :

- **clear conn** [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip* [*-src_ip*] [**netmask** *mask*]] [**port** *src_port* [*-src_port*]] [**address** *dest_ip* [*-dest_ip*] [**netmask** *mask*]] [**port** *dest_port* [*-dest_port*]]

  Cette commande met fin aux connexions, quel que soit leur état. Reportez-vous à la commande **show conn** pour afficher toutes les connexions actuelles.

  Sans arguments, cette commande efface toutes les connexions de transit. Pour effacer également les connexions vers la boîte (y compris votre session de gestion actuelle), utilisez le mot clé **all**. Pour effacer des connexions spécifiques en fonction de l'adresse IP source, de l'adresse IP de destination, du port et/ou du protocole, vous pouvez spécifier les options souhaitées.



CHAPITRE 3

Interface graphique utilisateur ASDM

Ce chapitre décrit comment utiliser l'interface graphique ASDM.

- À propos de l'interface utilisateur d'ASDM, à la page 53
- Navigation dans l'interface utilisateur d'ASDM, à la page 56
- Menus, à la page 57
- Barre d'outils, à la page 63
- Assistant ASDM, à la page 64
- Barre d'état, à la page 65
- Liste des périphériques, à la page 65
- Boutons communs, à la page 66
- Raccourcis clavier, à la page 67
- Trouver une fonction dans les volets ASDM, à la page 69
- Trouver une fonction dans les listes de règles, à la page 69
- Activation de la prise en charge étendue des lecteurs d'écran, à la page 70
- Dossier organisationnel, à la page 71
- Volet d'accueil (mode unique et contexte), à la page 71
- Volet d'accueil (système), à la page 85
- Définir les préférences ASDM, à la page 86
- Rechercher avec l'assistant ASDM, à la page 89
- Activation des mesures d'historique, à la page 89
- Commandes non prises en charge, à la page 90

À propos de l'interface utilisateur d'ASDM

L'interface utilisateur d'ASDM est conçue pour fournir un accès facile aux nombreuses fonctionnalités prises en charge par l'ASA. L'interface utilisateur d'ASDM comprend les éléments suivants :

- Une barre de menus qui permet d'accéder rapidement aux fichiers, aux outils, aux assistants et à l'aide. De nombreux éléments de menu ont également des raccourcis clavier.
- Une barre d'outils qui vous permet de naviguer dans ASDM. Dans la barre d'outils, vous pouvez accéder aux volets **Home** (Accueil), **Configuration** et **Monitoring** (Supervision). Vous pouvez également obtenir de l'aide et naviguer entre les volets.
- Un volet **Navigation** gauche ancrable permettant de parcourir les volets **Configuration** et **Monitoring** (Supervision). Vous pouvez cliquer sur l'un des trois boutons dans l'en-tête pour agrandir ou restaurer

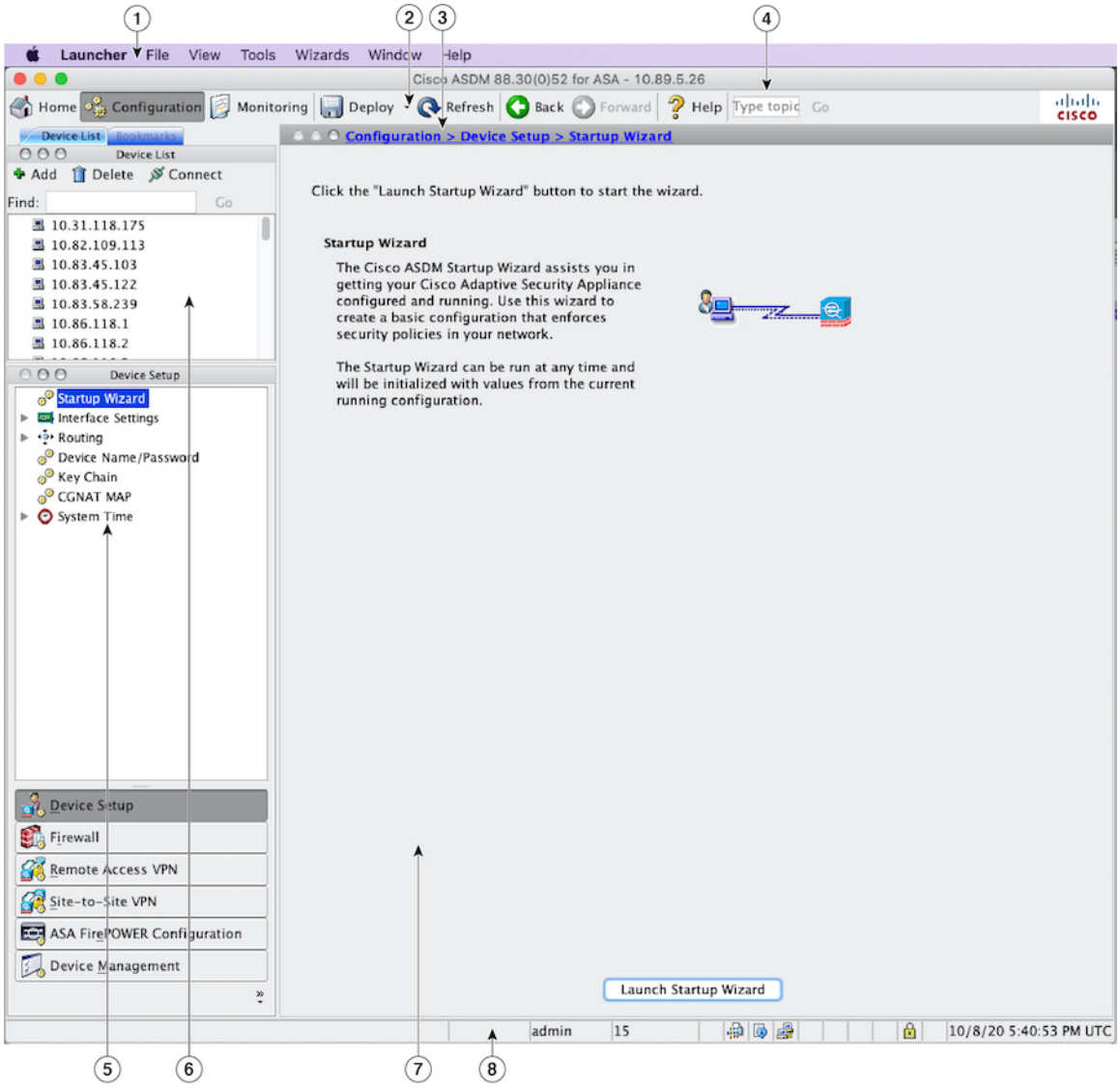
ce volet, en faire un volet flottant que vous pouvez déplacer, masquer ou fermer. Pour accéder aux volets **Configuration** et **Monitoring** (Supervision), vous pouvez effectuer l'une des opérations suivantes :

- Cliquez sur les liens sur le côté gauche de la fenêtre d'application dans le volet **de navigation** de gauche. Le volet **Content** (Contenu) affiche ensuite le chemin (par exemple, **Configuration > Device Setup (Configuration du périphérique) > Startup Wizard (Assistant de démarrage)**) dans la barre de titre du volet sélectionné.
- Si vous connaissez le chemin exact, vous pouvez le saisir directement dans la barre de titre du volet **Content** (Contenu) sur le côté droit de la fenêtre d'application, sans cliquer sur les liens dans le volet **Navigation** de gauche.

- Un bouton d'agrandir et de restaurer dans le coin droit du volet **Content** (Contenu) qui vous permet de masquer et d'afficher le volet **Navigation** de gauche.
- Un volet **Device List** (Liste des périphériques) ancrable avec une liste des périphériques auxquels vous pouvez accéder par l'intermédiaire d'ASDM. Vous pouvez cliquer sur l'un des trois boutons dans l'en-tête pour agrandir ou restaurer ce volet, en faire un volet flottant que vous pouvez déplacer, masquer ou fermer.
- Une barre d'état qui affiche l'heure, l'état de la connexion, l'utilisateur, l'état de la mémoire, l'état de configuration en cours, le niveau de privilège et l'état SSL au bas de la fenêtre d'application.
- Un volet **Navigation** de gauche qui affiche divers objets que vous pouvez utiliser dans les tableaux de règles lorsque vous créez des règles d'accès, des règles NAT, des règles AAA, des règles de filtrage et des règles de service. Les titres d'onglet dans le volet changent en fonction de la fonctionnalité que vous affichez. En outre, l'**assistant ASDM** apparaît dans ce volet.

La figure suivante montre les éléments de l'interface utilisateur d'ASDM.

Illustration 3 : Interface utilisateur d'ASDM



Légende

Élément d'interface graphique	Description
1	Barre de menus
2	Barre d'outils
3	Chemin de navigation
4	Zone de recherche

Élément d'interface graphique	Description
5	Volet de navigation gauche
6	Volet de liste des périphériques
7	Volet de contenu
8	Barre d'état



Remarque Des conseils d'outils ont été ajoutés pour diverses parties de l'interface graphique, notamment **les assistants**, les volets **de configuration** et **de supervision** et la **barre d'état**. Pour afficher les infobulles, placez le pointeur de la souris sur un élément précis de l'interface utilisateur, par exemple une icône dans la barre d'état.

Navigation dans l'interface utilisateur d'ASDM

Pour vous déplacer efficacement dans l'interface utilisateur ASDM, vous pouvez utiliser une combinaison de menus, la barre d'outils, les volets ancrables et les volets **de navigation** gauche et droit, qui sont décrits dans la section précédente. Les fonctions disponibles s'affichent dans une liste de boutons sous le volet **Device List** (Liste des périphériques). Un exemple de liste pourrait inclure les boutons de fonction suivants :

- **Configuration de l'appareil**
- **Pare-feu**
- **Filtre de trafic de réseau de zombies**
- **VPN d'accès à distance**
- **VPN de site à site**
- **Gestion des appareils**

La liste des boutons de fonction qui s'affiche est basée sur les fonctionnalités sous licence que vous avez achetées. Cliquez sur chaque bouton pour accéder au premier volet dans la fonction sélectionnée pour l'affichage de la configuration ou l'affichage de la surveillance. Les boutons de fonction ne sont pas disponibles dans l'affichage Home (Accueil).

Pour modifier l'affichage des boutons de fonction, procédez comme suit :

Procédure

Étape 1 Choisissez dans la liste déroulante sous le dernier bouton de fonction pour afficher un menu contextuel.

Étape 2 Choisissez une des options suivantes :

- Cliquez sur **Show More Buttons** (Afficher plus de boutons) pour afficher plus de boutons.

- Cliquez sur **Show Fewer Buttons** (Afficher moins de boutons) pour afficher moins de boutons.
- Cliquez sur **Add or Remove Buttons** (Ajouter ou supprimer des boutons) pour ajouter ou supprimer des boutons, puis cliquez sur le bouton à ajouter ou à supprimer dans la liste qui s'affiche.
- Choisissez **Option** pour afficher la boîte de dialogue **Option**, qui affiche une liste des boutons dans leur ordre actuel. Effectuez l'une des opérations suivantes :
  - Cliquez sur **Move Up** (Déplacer vers le haut) pour déplacer un bouton vers le haut dans la liste.
  - Cliquez sur **Move Down** (Déplacer vers le bas) pour déplacer un bouton vers le bas dans la liste.
  - Cliquez sur **Reset** (Réinitialiser) pour rétablir l'ordre des éléments dans la liste aux paramètres par défaut.

Étape 3 Cliquez sur **OK** pour enregistrer vos paramètres et fermer cette boîte de dialogue.

Menus

Vous pouvez accéder aux menus d'ASDM en utilisant la souris ou le clavier.

Menu Fichier

Le menu **File** (Fichier) vous permet de gérer les configurations ASA.

Élément de menu Fichier	Description
Reset Device to the Factory Default Configuration (Réinitialiser le périphérique à la configuration d'usine par défaut)	Charge une copie de la configuration en cours dans ASDM.
Reset Device to the Factory Default Configuration (Réinitialiser le périphérique à la configuration d'usine par défaut)	Rétablit les valeurs par défaut de la configuration.
Show Running Configuration in New Window (Afficher la configuration en cours d'exécution dans une nouvelle fenêtre)	Affiche la configuration en cours d'exécution dans une nouvelle fenêtre.
Save Running Configuration to Flash (Enregistrer la configuration en cours d'exécution dans la mémoire flash)	Écrit une copie de la configuration en cours dans la mémoire flash.

Élément de menu Fichier	Description
Save Running Configuration to TFTP Server (Enregistrer la configuration en cours d'exécution sur un serveur TFTP)	Stocke une copie du fichier de configuration en cours d'exécution sur un serveur TFTP.
Save Running Configuration to Standby Unit (Enregistrer la configuration en cours d'exécution sur l'unité de secours)	Envoie une copie du fichier de configuration en cours sur l'unité principale vers la configuration en cours d'une unité de secours de basculement.
Save Internal Log Buffer to Flash (Enregistrer le tampon de journal interne dans la mémoire flash)	Sauvegarde le tampon de journal interne dans la mémoire flash.
Deploy FirePOWER Changes (Déployer les modifications FirePOWER)	Enregistre les modifications de configuration apportées aux politiques de module ASA FirePOWER dans le module. Cette option est disponible uniquement si vous installez un module ASA FirePOWER et le gérez par l'intermédiaire d'ASDM.
Imprimer	Imprime la page actuelle. Nous vous recommandons d'utiliser une orientation de page paysage lorsque vous impression de règles. Lorsque vous utilisez Internet Explorer, l'autorisation d'impression a déjà été accordée lorsque vous avez initialement accepté l'Applet signé.
Clear ASDM Cache (Effacer le cache ASDM)	Supprime les images d'ASDM locales. ASDM télécharge les images localement lorsque vous vous connectez à ASDM.
Clear ASDM Password Cache (Effacer le cache du mot de passe ASDM)	Supprime le cache de mot de passe si vous avez défini un nouveau mot de passe et que vous avez toujours un mot de passe existant différent du nouveau mot de passe.
Clear Internal Log Buffer (Effacer le tampon de journalisation interne)	Vide le tampon du message syslog.
Quitter	Ferme ASDM.

Menu d'affichage

Le menu **View** (Affichage) vous permet d'afficher diverses parties de l'interface utilisateur d'ASDM. Certains éléments dépendent de l'affichage actuel. Vous ne pouvez pas sélectionner d'éléments qui ne peuvent pas être affichés dans l'affichage actuel.

Élément du menu View (Affichage)	Description
Accueil	Affiche la vue Home (Accueil).
Configuration	Affiche la vue Configuration.
Monitoring (Surveillance)	Affiche la vue Monitoring (Supervision).

Élément du menu View (Affichage)	Description
Signets	Affiche une liste des pages mises en signet dans un volet ancrable.
Liste des périphériques	Affiche une liste des périphériques dans un volet ancrable.
Navigation	Affiche et masque le volet **Navigation** dans les vues Configuration et Monitoring (Supervision).
ASDM Assistant (Assistant ASDM)	Recherche et trouve l'aide procédurale d'ASDM utile concernant certaines tâches.
Latest ASDM Syslog Messages (Derniers messages Syslog ASDM)	Affiche et masque le volet **Latest ASDM Syslog Messages** (Derniers messages Syslog ASDM) dans la vue Home (Accueil). Ce volet est uniquement disponible dans la vue Home (Accueil). Si vous ne disposez pas de mémoire suffisante pour effectuer la mise à niveau vers la version la plus actuelle, le message syslog %ASA-1-211004 est généré, indiquant la mémoire installée et la mémoire requise. Ce message réapparaît toutes les 24 heures jusqu'à ce que la mémoire soit mise à niveau.
Adresses	Affiche et masque le volet **Addresses**. Le volet **Adresses** est uniquement disponible pour les volets **Access Rules** (Règles d'accès), **NAT Rules** (Règles NAT), **Service Policy Rules** (Règles de politique de service), **AAA Rules** (Règles AAA) et **Filter Rules** (Règles de filtrage) dans la vue Configuration.
Services	Affiche et masque le volet **Services**. Le volet **Services** est uniquement disponible pour les volets **Access Rules** (Règles d'accès), **NAT Rules** (Règles NAT), **Service Policy Rules** (Règles de politique de service), **AAA Rules** (Règles AAA) et **Filter Rules** (Règles de filtrage) dans la vue Configuration.
Plages de temps	Affiche et masque le volet **Time Ranges** (Plages temporelles). Le volet **Time Ranges** (Plages temporelles) est uniquement disponible pour les volets **Access Rules** (Règles d'accès), **Service Policy Rules** (Règles de politique de service), **AAA Rules** (Règles AAA) et **Filter Rules** (Règles de filtrage) dans la vue Configuration.
Select Next Pane (Sélectionner le volet suivant)	Met en surbrillance le volet suivant affiché dans une vue à plusieurs volets, par exemple, en passant du volet Service Policy Rules (Règles de politique de service) au volet Addresses situé à côté.
Select Previous Pane (Sélectionner le volet précédent)	Met en surbrillance le volet précédent affiché dans les affichages à volets multiples.
Retour	Retourne au volet précédent.
Rediriger	Passe au volet suivant précédemment visité.
Find in ASDM (Trouver dans ASDM)	Localise l'élément recherché, par exemple une fonctionnalité ou l'**Assistant ASDM**.

Élément du menu View (Affichage)	Description
Reset Layout (Réinitialiser la disposition)	Restaure la disposition à la configuration par défaut.
Office Look and Feel (Apparence et convivialité du bureau)	Remplace les polices et les couleurs d'écran par les paramètres Microsoft Office.

Menu Outils

Le menu **Tools** (Outils) vous fournit les séries d'outils suivantes à utiliser dans ASDM.

Élément de menu Outils	Description
Interface de commande en ligne	Envoie des commandes à l'ASA et affiche les résultats.
Afficher les commandes ignorées par ASDM sur l'appareil	Affiche les commandes non prises en charge qui ont été ignorées par ASDM.
Packet Tracer	Effectue le suivi d'un paquet à partir d'une adresse source et d'une interface source spécifiées vers une destination. Vous pouvez préciser le protocole et le port de n'importe quel type de données et afficher la durée de vie d'un paquet, avec des informations détaillées sur les actions qui lui sont appliquées. Consultez le guide de configuration du pare-feu pour plus d'informations.
Ping	Vérifie la configuration et le fonctionnement de l'appareil de sécurité adaptable Cisco et des liens de communication environnants, en plus d'effectuer des tests de base sur d'autres appareils réseau. Consultez le guide de configuration du pare-feu pour plus d'informations.
Traceroute	Détermine la route que les paquets emprunteront pour atteindre leur destination. Consultez le guide de configuration du pare-feu pour plus d'informations.
Gestion des fichiers	Affiche, déplace, copie et supprime les fichiers stockés dans la mémoire flash. Vous pouvez également créer un répertoire dans la mémoire flash. Vous pouvez également transférer des fichiers entre différents systèmes de fichiers, y compris TFTP, mémoire flash et votre PC local.
Vérifier les mises à jour d'ASA/ASDM	Met à niveau le logiciel ASA et le logiciel ASDM à l'aide d'un assistant.
Mise à niveau du logiciel à partir de l'ordinateur local	Charge une image ASA, une image ASDM ou une autre image de votre PC vers la mémoire flash.
Rétrograder le logiciel	Charge une image ASA plus ancienne que celle que vous utilisez actuellement.
Sauvegarder les configurations	Sauvegarde la configuration ASA, une image Cisco Secure Desktop ainsi que les images et les profils de clients VPN SSL.

Élément de menu Outils	Description
Restaurer les configurations	Restaure la configuration ASA, une image Cisco Secure Desktop ainsi que les images et les profils de clients VPN SSL.
Rechargement du système	Redémarre l'ASDM et recharge la configuration enregistrée dans la mémoire.
Alerte de l'administrateur pour les utilisateurs de VPN SSL sans client	Permet à un administrateur d'envoyer un message d'alerte aux utilisateurs de VPN SSL sans client. Consultez le guide de configuration de VPN pour en savoir plus.
Migrer les membres du groupe d'objets réseau	Si vous migrez vers la version 8.3 ou une version ultérieure, l'ASA crée des objets réseau nommés pour remplacer les adresses IP en ligne dans certaines fonctionnalités. En plus des objets nommés, ASDM crée automatiquement des objets non nommés pour toutes les adresses IP utilisées dans la configuration. Ces objets créés automatiquement sont identifiés par l'*adresse IP* uniquement, n'ont pas de nom et ne sont pas présents en tant qu'objets nommés dans la configuration de la plateforme. Lorsque l'ASA crée des objets nommés dans le cadre de la migration, les objets correspondants non nommés d'ASDM uniquement sont remplacés par les objets nommés. La seule exception concerne les objets sans nom dans un groupe d'objets réseau. Lorsque l'ASA crée des objets nommés pour les adresses IP qui se trouvent dans un groupe d'objets réseau, ASDM conserve les objets non nommés, ce qui crée des objets en double dans ASDM. Choisissez **Tools (Outils) > Migrate Network Object Group Members** (Migrer les membres du groupe d'objets réseau) pour fusionner ces objets. Consultez la section *Migration de Cisco ASA 5500 vers la version 8.3 et les versions ultérieures* pour en savoir plus.
Préférences	Modifie le comportement des fonctions ASDM spécifiées entre les sessions.
Console Java ASDM	Affiche la console Java.

Menu Wizards (Assistants)

Le menu **Wizards** (Assistants) vous permet d'exécuter un assistant pour configurer plusieurs fonctionnalités.

Élément de menu Wizards (Assistants)	Description
Assistant de démarrage	Vous guide, étape par étape, dans la configuration initiale de l'ASA.
Assistants VPN	Il existe des assistants distincts pour une variété de configurations VPN. Consultez le guide de configuration de VPN pour en savoir plus.
Assistant de haute accessibilité et d'évolutivité	Vous permet de configurer le basculement : l'équilibrage de charges de grappe VPN ou la mise en grappe ASA sur l'ASA.

Élément de menu Wizards (Assistants)	Description
Assistant de communications unifiées	Vous permet de configurer des fonctionnalités de communication unifiée, comme un téléphone IP, sur l'ASA. Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements.
Assistant de certificat d'identité ASDM	Lorsque vous utilisez la mise à jour 51 de Java 7 et les versions ultérieures, le lanceur ASDM nécessite un certificat de confiance. Une méthode simple pour répondre aux exigences en matière de certificats consiste à installer un certificat d'identité autosigné. Vous pouvez utiliser Java Web Start pour lancer ASDM jusqu'à ce que vous installiez un certificat à l'aide de cet assistant. Consultez le site http://www.cisco.com/go/asdm-certificate pour en savoir plus.
Assistant de capture de paquets	Vous permet de configurer la capture de paquets sur l'ASA. L'assistant exécute une capture de paquets sur chacune des interfaces d'entrée et de sortie. Après avoir exécuté la capture, vous pouvez l'enregistrer sur votre ordinateur, puis examiner et analyser la capture à l'aide d'un analyseur de paquets.

Menu de la fenêtre

Le menu **Window** (Fenêtre) vous permet de vous déplacer entre les fenêtres ASDM. La fenêtre active s'affiche comme fenêtre sélectionnée.

Menu d'aide

Le menu **Help** (Aide) fournit des liens vers de l'aide en ligne, ainsi que des renseignements sur ASDM et l'ASA.

Éléments de menu d'aide	Description
Rubriques d'aide	Ouvre une nouvelle fenêtre de navigateur pour afficher l'aide en ligne d'ASDM. Si vous gérez un module ASA FirePOWER dans ASDM, cet élément est étiqueté **ASDM Help Topics** (Rubriques d'aide d'ASDM).
ASA FirePOWER Help Topics (Rubriques d'aide d'ASA FirePOWER)	Ouvre une nouvelle fenêtre de navigateur pour afficher l'aide en ligne du module ASA FirePOWER. Cet élément est disponible uniquement si vous avez installé le module et que vous le gérez dans ASDM.
Help for Current Screen (Aide pour l'écran actuel)	Ouvre l'aide contextuelle de l'écran que vous consultez. Sinon, vous pouvez également cliquer sur le **? Bouton Help (Aide)** dans la barre d'outils.
Notes de mise à jour	Ouvre la version la plus actuelle des *notes de mise à jour d'ASDM* sur Cisco.com. Les notes de mise à jour contiennent les renseignements les plus à jour sur les exigences du logiciel et du matériel d'ASDM, ainsi que les renseignements les plus à jour sur les modifications apportées au logiciel.

Éléments de menu d'aide	Description
Cisco ASA Series Documentation (Documentation de la série ASA de Cisco)	Ouvre un document sur Cisco.com qui comprend des liens vers toute la documentation de produit disponible.
ASDM Assistant (Assistant ASDM)	Ouvre l'**assistant ASDM**, qui vous permet de rechercher du contenu téléchargeable à partir de Cisco.com, avec des détails sur l'exécution de certaines tâches.
About Cisco Adaptive Security Appliance (ASA) [À propos de Cisco Adaptive Security Appliance (ASA)]	Affiche les renseignements sur l'ASA, y compris la version du logiciel, l'ensemble de matériel, le fichier de configuration chargé au démarrage et l'image logicielle chargée au démarrage. Ces renseignements aident au dépannage.
About Cisco ASDM (À propos de Cisco ASDM)	Affiche les informations sur ASDM telles que la version du logiciel, le nom d'hôte, le niveau de privilège, le système d'exploitation, le type de périphérique et la version de Java.

Barre d'outils

La **Barre d'outils** sous les menus permet d'accéder aux affichages Home (Accueil), Configuration et Monitoring (Surveillance). Il vous permet également de choisir entre les contextes système et de sécurité en mode contexte multiple, et fournit la navigation et d'autres fonctionnalités couramment utilisées.

Bouton de la barre d'outils	Description
Accueil	Affiche le volet **Home** (Accueil), qui vous permet d'afficher des informations importantes sur votre ASA telles que l'état de vos interfaces, la version que vous utilisez, les renseignements de licence et les performances. En mode multiple, le système n'a pas de volet Home (Accueil).
Configuration	Configure l'ASA. Cliquez sur un bouton de fonction dans le volet **Navigation** de gauche pour configurer cette fonction.
Monitoring (Surveillance)	Surveille l'ASA. Cliquez sur un bouton de fonction dans le volet **Navigation** de gauche pour surveiller divers éléments.
Enregistrer	Enregistre la configuration en cours d'exécution dans la configuration de démarrage pour les contextes accessibles en écriture uniquement. Le bouton est remplacé par le bouton **Deploy** (Déployer) si un module ASA FirePOWER est installé sur le périphérique et que vous le configurez par le biais d'ASDM.

Bouton de la barre d'outils	Description
Déployer	Si un module ASA FirePOWER est installé sur le périphérique et que vous le configurez par le biais d'ASDM, le bouton **Deploy** (Déployer) remplace le bouton **Save** (Enregistrer) et contient les options suivantes : • **Deploy FirePOWER Changes** (Déployer les modifications FirePOWER) : enregistre les modifications de configuration apportées aux politiques de module ASA FirePOWER dans le module. • **Save Running Configuration to Flash** (Enregistrer la configuration en cours dans la mémoire flash) : écrit une copie de la configuration de l'ASA en cours dans la mémoire flash. Cela équivaut au bouton **Save** (Enregistrer) pour les périphériques qui ne comprennent pas de module ASA FirePOWER.
Actualiser	Actualise ASDM avec la configuration actuelle en cours d'exécution, à l'exception des graphiques dans les volets Monitoring (Surveillance).
Retour	Retourne au dernier volet d'ASDM que vous avez visité.
Rediriger	Passe au dernier volet d'ASDM que vous avez visité.
Aide	Affiche l'aide contextuelle pour l'écran actuellement ouvert.
Rechercher	Recherche une fonctionnalité dans ASDM. La fonction de recherche parcourt les titres de chaque volet et vous présente une liste de correspondances et vous donne un lien hypertexte directement vers ce volet. Cliquez sur **Back** (Précédent) ou **Forward** (Suivant) pour basculer rapidement entre les deux volets différents que vous avez trouvés.

Assistant ASDM

L'assistant ASDM vous permet de rechercher et d'afficher une aide procédurale utile d'ASDM concernant certaines tâches. Cette fonctionnalité est disponible en modes routé et transparent, ainsi que dans les contextes unique et système.

Choisissez **View (Afficher)** > **ASDM Assistant (Assistant ASDM)** > **How Do I? (Comment faire?)** ou saisissez une demande de recherche dans le champ **Look For (Rechercher)** de la barre de menus pour accéder aux informations. Choisissez **How Do I?** (Comment faire?) dans la liste déroulante **Find** (Chercher) pour commencer la recherche.

Pour utiliser l'assistant ASDM, procédez comme suit :

Procédure

Étape 1 Choisissez **View (Afficher)** > **ASDM Assistant (Assistant ASDM)**.

Le volet **ASDM Assistant** (Assistant ASDM) apparaît.

Étape 2 Saisissez les informations que vous souhaitez trouver dans le champ **Search** (Rechercher), puis cliquez sur **Go** (Aller).

Les informations demandées s'affichent dans le volet **Search Results** (Résultats de la recherche).

Étape 3 Cliquez sur les liens qui apparaissent dans les sections **Search Results (Résultats de la recherche) et Features (Fonctionnalités)** pour obtenir plus de détails.

Barre d'état

La **barre d'état** apparaît au bas de la fenêtre ASDM. Le tableau suivant répertorie les zones affichées de gauche à droite.

Domaine	Description
État	L'état de la configuration (par exemple, « Configuration du périphérique chargée avec succès »).
Basculement	L'état de l'unité de basculement, qu'elle soit active ou en veille.
Nom d'utilisateur	Le nom d'utilisateur de l'ASDM. Si vous vous êtes connecté sans nom d'utilisateur, le nom d'utilisateur est « admin ».
Privilège d'utilisateur	Le privilège de l'utilisateur ASDM.
Commandes ignorées par ASDM	Cliquez sur l'icône pour afficher une liste des commandes de votre configuration qu'ASDM n'a pas traitées. Ces commandes ne seront pas supprimées de la configuration.
Connexion au périphérique	L'état de la connexion de l'ASDM à l'ASA.
Connexion Syslog	La connexion au syslog est activée et l'ASA est surveillée.
SSL sécurisé	La connexion à ASDM est sécurisée, car elle utilise SSL.
Le temps,	L'heure définie sur l'ASA.

Connexion au périphérique

ASDM maintient une connexion permanente avec l'ASA pour maintenir à jour les données des volets **Monitoring** (Supervision) et **Home** (Accueil). Cette boîte de dialogue affiche l'état de la connexion. Lorsque vous apportez une modification de configuration, ASDM ouvre une deuxième connexion pour la durée de la configuration, puis la ferme; cependant, cette boîte de dialogue ne représente pas la deuxième connexion.

Liste des périphériques

La liste des périphériques est un volet ancrable. Vous pouvez cliquer sur l'un des trois boutons dans l'en-tête pour agrandir ou restaurer ce volet, en faire un volet flottant que vous pouvez déplacer, masquer ou fermer.

Ce volet est disponible dans les vues Accueil, Configuration, Supervision et Système. Vous pouvez utiliser ce volet pour passer à un autre périphérique et entre le système et les contextes; cependant, ce périphérique doit exécuter la même version d'ASDM que vous utilisez actuellement. Pour afficher le volet entièrement, vous devez avoir au moins deux périphériques répertoriés. Ce volet est disponible en modes routé et transparent, et dans les contextes unique, multiple et système.

Pour utiliser ce volet afin de vous connecter à un autre périphérique, procédez comme suit :

Procédure

Étape 1 Cliquez sur **Add** (Ajouter) pour ajouter un autre périphérique à la liste.

La boîte de dialogue **Add Device** (Ajouter un périphérique) apparaît.

Étape 2 Saisissez le nom de périphérique ou l'adresse IP du périphérique, puis cliquez sur **OK**.

Étape 3 Cliquez sur **Delete** (Supprimer) pour supprimer un périphérique sélectionné de la liste.

Étape 4 Cliquez sur **Connect** (Connecter) pour vous connecter à un autre périphérique.

La boîte de dialogue **Enter Network Password** (Entrer le mot de passe réseau) apparaît.

Étape 5 Saisissez votre nom d'utilisateur et votre mot de passe dans les champs appropriés, puis cliquez sur **Login** (Connexion).

Boutons communs

De nombreux volets d'ASDM comprennent des boutons répertoriés dans le tableau suivant. Cliquez sur le bouton applicable pour effectuer la tâche souhaitée :

Bouton	Description
Appliquer	Envoie les modifications apportées dans ASDM à l'ASA et les applique à la configuration en cours d'exécution.
Enregistrer	Enregistre une copie de la configuration en cours d'exécution dans la mémoire flash.
Réinitialiser	Annule les modifications et rétablit les informations affichées avant les modifications ou lors du dernier clic sur Refresh (Actualiser) ou Apply (Appliquer). Après avoir cliqué sur **Reset** (Réinitialiser), cliquez sur **Refresh** (Actualiser) pour vous assurer que les informations de la configuration en cours d'exécution s'affichent.
Rétablir les paramètres par défaut	Efface les paramètres sélectionnés et rétablit les paramètres par défaut.
Annuler	Annule les modifications et revient au volet précédent.
Enable (activer)	Affiche les statistiques en lecture seule d'une fonctionnalité.
Fermer	Ferme une boîte de dialogue ouverte.

Bouton	Description
Effacer	Supprime les informations d'un champ ou décoche une case.
Retour	Revient au volet précédent.
Rediriger	Passe au volet suivant.
Aide	Affiche l'aide relative au volet ou à la boîte de dialogue sélectionné.

Raccourcis clavier

Vous pouvez utiliser le clavier pour naviguer dans l'interface utilisateur d'ASDM.

Le tableau suivant répertorie les raccourcis clavier que vous pouvez utiliser pour vous déplacer dans les trois zones principales de l'interface utilisateur d'ASDM.

Tableau 2 : Raccourcis clavier dans la fenêtre principale

Pour afficher le	Windows/Linux	MacOS
Volet**d'accueil**	Ctrl+H	Shift+Command+H
Volet **de configuration**	Ctrl+G	Shift+Command+G
Volet de **supervision**	Ctrl+M	Shift+Command+M
Aide	F1	Command+?
Retour	Alt+Left Arrow	Command+[
Rediriger	Alt+Rightarrow	Command+]
Actualiser l'affichage	F5	Command+R
Coupez	Ctrl+X	Command+X
Copier	Ctrl+C	Command+C
Coller	Ctrl+V	Command+V
Enregistrer la configuration	Ctrl+S	Command+S
Menus contextuels	Shift+F10	—
Fermer une fenêtre secondaire	Alt+F4	Command+W
Rechercher	Ctrl+F	Command+F
Quitter	Alt+F4	Command+Q
Quitter un tableau ou une zone de texte	Ctrl_Shift ou Ctrl+Shift+Tab	Ctril+Shift ou Ctrl+Shift+Tab

Le tableau suivant répertorie le raccourci clavier que vous pouvez utiliser pour naviguer dans un volet.

Tableau 3 : Raccourcis clavier dans un volet

Pour déplacer la mise au point sur	Cliquez sur
Champ suivant	Onglet
Champ précédent	Shift+Tab
Champ suivant lorsque le centre d'intérêt est dans un tableau	Ctrl+Tab
Champ précédent lorsque le centre d'intérêt est dans un tableau	Shift+Ctrl+Tab
Onglet **Suivant** (lorsqu'un onglet a le centre d'intérêt)	Flèche vers la droite
Onglet **Précédent** (lorsqu'un onglet a le centre d'intérêt)	Flèche vers la gauche
Cellule suivante dans un tableau	Onglet
Cellule précédente dans un tableau	Shift+Tab
Volet suivant (lorsque plusieurs volets sont affichés)	F6
Volet précédent (lorsque plusieurs volets sont affichés)	Shift+F6

Le tableau suivant répertorie les raccourcis clavier que vous pouvez utiliser avec les visualiseurs de journaux.

Tableau 4 : Raccourcis clavier pour la visualisation du journal

Destinataire	Windows/Linux	MacOS
Suspendre et reprendre la visualisation du journal en temps réel	Ctrl+U	Command+
Actualiser le volet du tampon de journalisation	F5	Command+R
Effacer le tampon de journalisation interne	Ctrl+Delete	Command+Delete
Copier l'entrée de journal sélectionnée	Ctrl+C	Command+C
Enregistrer le journal	Ctrl+S	Command+S
Impression	Ctrl+P	Command+P
Fermer une fenêtre secondaire	Alt+F4	Command+W

Le tableau suivant répertorie les raccourcis clavier que vous pouvez utiliser pour accéder aux éléments de menu.

Tableau 5 : Raccourcis clavier pour accéder aux éléments de menu

Pour accéder à	Windows/Linux
Barre de menus	Alt

Pour accéder à	Windows/Linux
Menu suivant	Flèche vers la droite
Menu précédent	Flèche vers la gauche
Option de menu suivante	Flèche vers le bas
Option de menu précédente	Flèche vers le haut
Option de menu sélectionnée	Saisissez

Trouver une fonction dans les volets ASDM

Certains volets d'ASDM contiennent des tableaux avec de nombreux éléments. Pour vous permettre de rechercher, de mettre en surbrillance puis de modifier une entrée particulière, plusieurs volets d'ASDM ont une fonction de recherche qui vous permet de rechercher des objets dans ces volets.

Pour effectuer une recherche, vous pouvez saisir une phrase dans le champ Find (Rechercher) pour effectuer une recherche dans toutes les colonnes d'un volet donné. La phrase peut contenir les caractères génériques « * » et « ? ». Le * correspond à un ou plusieurs caractères, et ? correspond à un caractère unique. Les flèches vers le haut et vers le bas à droite du champ **Find** (Rechercher) localisent respectivement l'occurrence suivante (haut) ou précédente (bas) de la phrase. Cochez la case **Match Case** (Respecter la casse) pour trouver les entrées correspondant exactement aux majuscules et minuscules saisies.

Par exemple, la saisie de B*ton-L* peut renvoyer les correspondances suivantes :

```
Boston-LA, Boston-Lisbon, Boston-London
```

La saisie de Bo?ton peut renvoyer les correspondances suivantes :

```
Boston, Bolton
```

Trouver une fonction dans les listes de règles

Comme les ACL et ACE et d'autres règles contiennent de nombreux éléments de types différents, la fonction de recherche dans tout volet qui affiche des règles permet une recherche plus ciblée que la fonction de recherche dans les autres volets. Cela inclut les règles d'accès, les règles de politique de service, le gestionnaire d'ACL et tout autre volet qui répertorie les règles d'ACL, ainsi que les règles de NAT.

Pour trouver des éléments dans les listes de règles, procédez comme suit :

Procédure

Étape 1 Cliquez sur **Find** (Rechercher).

Étape 2 Choisissez l'une des options suivantes dans le champ **Filter** (Filtre) de la liste déroulante.

Les éléments sur lesquels vous pouvez effectuer une recherche varient selon le type de règle et correspondent aux colonnes du tableau. Sélectionnez **Query** (Requête) si vous souhaitez créer une recherche complexe utilisant plusieurs champs.

Étape 3 À moins d'avoir sélectionné **Query** (Requête), choisissez dans le deuxième champ l'une des options suivantes dans la liste déroulante :

- **is** (est) : spécifie une correspondance exacte avec la chaîne de recherche. Il s'agit toujours de l'option pour les requêtes.
- **contains** (contient) : spécifie une correspondance avec toute règle qui contient, exactement ou partiellement, votre chaîne de recherche.

Étape 4 Dans le troisième champ, saisissez la chaîne que vous souhaitez trouver. Cliquez sur **...** pour choisir un objet dans une liste. Si vous utilisez une requête, cliquez sur **Define Query** (Définir la requête).

Si vous recherchez une adresse IP, vous pouvez obtenir des correspondances avec les adresses qui se trouvent dans un objet ou un groupe de réseau, tant que cet objet ou ce groupe a été créé par ASDM. C'est-à-dire que le nom du groupe commence par DM_INLINE. La fonctionnalité de recherche ne peut pas trouver les adresses IP dans les objets créés par l'utilisateur.

Étape 5 Cliquez sur **Filter** (Filtrer) pour effectuer la recherche.

L'affichage est mis à jour pour n'afficher que les règles qui correspondent. Les numéros de règles sont conservés afin que vous puissiez voir leur emplacement absolu dans la liste de règles.

Étape 6 Cliquez sur **Clear** (Effacer) pour supprimer le filtre et afficher de nouveau la liste complète.

Étape 7 Lorsque vous avez terminé, cliquez sur le **x** rouge pour fermer les contrôles de recherche.

Activation de la prise en charge étendue des lecteurs d'écran

Par défaut, les étiquettes et les descriptions ne sont pas incluses dans l'ordre des tabulations lorsque vous appuyez sur la touche **Tabulation** pour naviguer dans un volet. Certains logiciels de lecture d'écran, comme JAWS, lisent uniquement les objets écrans qui ont la mise au point. Vous pouvez inclure les étiquettes et les descriptions dans l'ordre des onglets en activant la prise en charge étendue du lecteur d'écran.

Pour activer la prise en charge étendue des lecteurs d'écran, procédez comme suit :

Procédure

Étape 1 Choisissez **Tools (Outils)** > **Preferences (Préférences)**.

La boîte de dialogue **Preferences** (Préférences) s'affiche.

Étape 2 Cochez la case **Enable screen reader support** (Activer la prise en charge du lecteur d'écran) sous l'onglet **General** (Général).

Étape 3 Cliquez sur **OK**.

Étape 4 Redémarrez ASDM pour activer la prise en charge du lecteur d'écran.

Dossier organisationnel

Certains dossiers dans le volet de navigation pour les affichages de configuration et de supervision ne sont pas associés à des volets de configuration ou de supervision. Ces dossiers sont utilisés pour organiser les tâches de configuration et de supervision associées. Cliquez sur ces dossiers pour afficher une liste de sous-éléments dans le volet **Navigation** de droite. Vous pouvez cliquer sur le nom d'un sous-élément pour accéder à cet élément.

Volet d'accueil (mode unique et contexte)

Le volet **Home** (Accueil) d'ASDM vous permet d'afficher des informations importantes sur votre ASA. Les informations sur l'état dans le volet **Home** (Accueil) sont mises à jour toutes les dix secondes. Ce volet comporte généralement deux onglets : **Device Dashboard** (Tableau de bord du périphérique) et **Firewall** Dashboard (Tableau de bord du pare-feu).

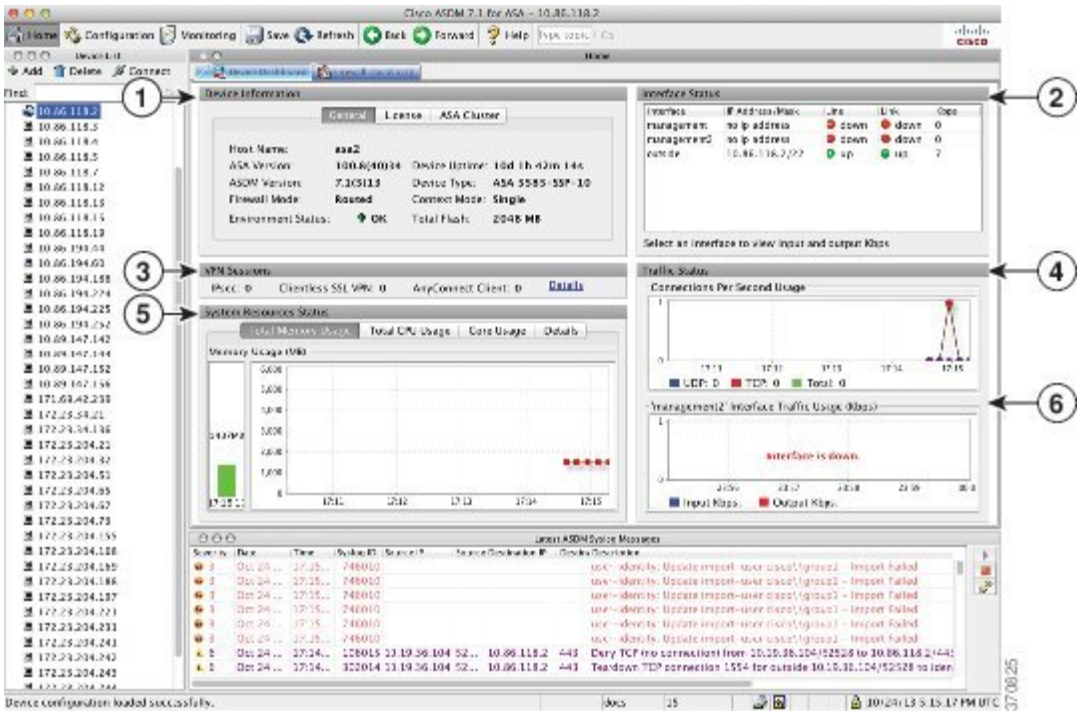
Si des modules de matériel ou de logiciel sont installés sur le périphérique, comme les modules IPS, CX ou ASA FirePOWER, il y a des onglets distincts pour ces modules.

Onglet Device Dashboard (Tableau de bord des périphériques)

L'onglet **Device Dashboard** (Tableau de bord des périphériques) vous permet d'afficher, en un coup d'œil, des informations importantes sur votre périphérique de sécurité adaptable Cisco, telles que l'état de vos interfaces, la version que vous utilisez, les renseignements de licence et les performances.

La figure suivante montre les éléments de l'onglet **Device Dashboard** (Tableau de bord des périphériques).

Illustration 4 : Onglet Device Dashboard (Tableau de bord des périphériques)



Légende

Élément de GUI	Description
1	Volet Device Information (Informations sur le périphérique), à la page 72
2	Volet d'état de l'interface, à la page 74
3	Volet des sessions VPN, à la page 74
4	Panneau de l'état du trafic, à la page 74
5	Volet d'état des ressources système, à la page 74
6	Panneau de l'état du trafic, à la page 74
—	Liste des périphériques, à la page 65
—	Derniers messages Syslog d'ASDM, à la page 75

Volet Device Information (Informations sur le périphérique)

Le volet **Device Information** (Informations sur le périphérique) comprend deux onglets qui affichent les informations sur le périphérique : l'onglet **General** (Général) et l'onglet **License** (Licence). Sous l'onglet **General** (Général), vous avez accès au bouton **Environment Status** (État de l'environnement), qui fournit une vue d'ensemble de l'état du système :

Onglet Général

Cet onglet affiche les informations de base sur l'ASA :

- **Host name** (Nom de domaine) : affiche le nom de domaine du périphérique.
- **ASA version** (Version ASA) : répertorie la version du logiciel ASA qui est exécutée sur le périphérique.
- **ASDM version** (Version ASDM) : répertorie la version du logiciel d'ASDM qui est exécutée sur le périphérique.
- **Firewall mode** (Mode pare-feu) : affiche le mode de pare-feu dans lequel le périphérique fonctionne.
- **Total flash** (Mémoire flash totale) : affiche la quantité totale de RAM actuellement utilisée.
- **ASA Cluster Role** (Rôle dans la grappe ASA) : lorsque vous activez la mise en grappe, affiche le rôle de cette unité, qu'elle soit matrice ou esclave.
- **Device uptime (Durée de fonctionnement du périphérique)** : affiche la durée pendant laquelle le périphérique a été opérationnel depuis le dernier chargement de logiciel.
- **Context mode** (Mode contexte) : affiche le mode contexte dans lequel le périphérique fonctionne.
- **Total Memory** (Mémoire totale) : affiche la DRAM installée sur l'ASA.
- **Environment status** (État de l'environnement) : affiche l'intégrité du système. Affichez les statistiques matérielles en cliquant sur le signe plus (+) à droite de l'étiquette **Environment Status** (État de l'environnement) dans l'onglet **General** (Général). Vous pouvez voir le nombre de blocs d'alimentation installés, suivre l'état opérationnel des modules de ventilation et des blocs d'alimentation, ainsi que les températures des CPU et la température ambiante du système.

  En général, le bouton **Environment Status** (État de l'environnement) fournit une vue d'ensemble de l'intégrité du système. Si tous les composants matériels supervisés du système fonctionnent dans des plages normales, le bouton du signe plus (+) affiche OK en vert. Inversement, si un composant du système matériel fonctionne en dehors des plages normales, le bouton du signe plus (+) devient un cercle rouge pour afficher l'état Critical (Critique) et indiquer qu'un composant matériel nécessite une intervention immédiate.

  Consultez le guide du matériel de votre périphérique pour obtenir plus d'informations sur les statistiques matérielles.



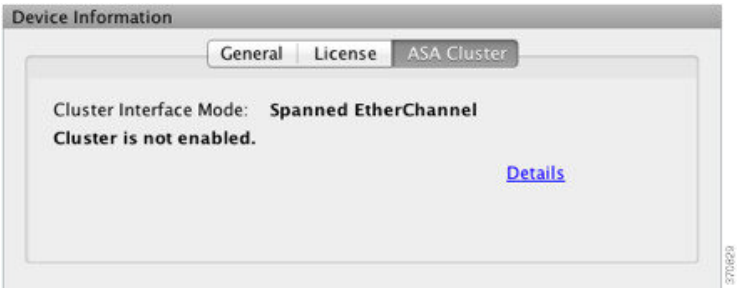
Remarque Si vous ne disposez pas de suffisamment de mémoire pour effectuer la mise à niveau vers la version la plus récente de l'ASA, la boîte de dialogue **Memory Insufficient Warning** (Avertissement de mémoire insuffisante) s'affiche. Suivez les instructions qui s'affichent dans cette boîte de dialogue pour continuer à utiliser l'ASA et l'ASDM d'une manière prise en charge. Cliquez sur **OK** pour fermer cette boîte de dialogue.

Onglet Licences

Cet onglet affiche un sous-ensemble de fonctionnalités sous licence. Cliquez sur **More Licenses** (Plus de licences) pour afficher des informations détaillées sur les licences ou saisir une nouvelle clé d'activation; le volet **Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Activation Key (Clé d'activation)** s'affiche.

Onglet Cluster (Grappe)

Cet onglet affiche le mode d'interface de grappe ainsi que l'état de la grappe.



Onglet Ressources virtuelles (ASAv)

Cet onglet affiche les ressources virtuelles utilisées par l ASA virtuel, y compris le nombre de vCPU, de RAM et si l ASA virtuel est surprovisionné ou sous-provisionné.

Volet d'état de l'interface

Ce volet affiche l'état de chaque interface. Si vous sélectionnez une ligne d'interface, les débits d'entrée et de sortie en Kbit/s s'affichent sous le tableau.

Volet des sessions VPN

Ce volet affiche l'état du tunnel VPN. Cliquez sur **Details** (Détails) pour accéder au volet **Monitoring (Supervision) > VPN > VPN Statistics (Statistiques VPN) > Sessions**.

Volet d'état de basculement

Ce volet affiche l'état du basculement.

Cliquez sur **Configure** (Configurer) pour démarrer l'assistant Haute accessibilité et évolutivité. Une fois l'assistant terminé, l'état de la configuration de basculement (actif/actif ou actif/veille) s'affiche.

Si le basculement est configuré, cliquez sur Details (**Détails**) pour ouvrir le volet **Monitoring (Surveillance) > Properties (Propriétés) > Failover (Basculement) > Status (État)**.

Volet d'état des ressources système

Ce volet affiche les statistiques d'utilisation du CPU et de la mémoire.

Panneau de l'état du trafic

Ce volet affiche des graphiques pour les connexions par seconde pour toutes les interfaces et pour le débit du trafic de l'interface de sécurité la plus basse.

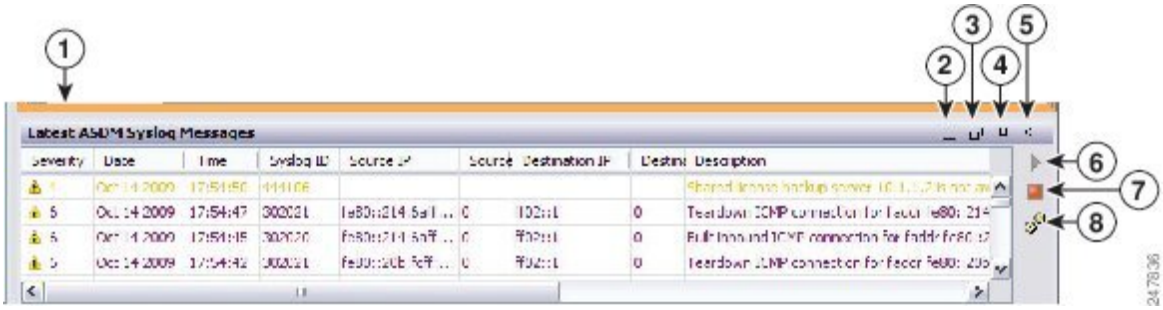
Lorsque votre configuration contient plusieurs interfaces de niveau de sécurité le plus bas et que l'une d'entre elles est nommée « outside » (externe), cette interface est utilisée pour les graphiques de débit du trafic. Sinon, ASDM choisit la première interface dans la liste alphabétique des interfaces de niveau de sécurité le plus bas.

Derniers messages Syslog d'ASDM

Ce volet affiche les plus récents messages système générés par l'ASA, jusqu'à un maximum de 100 messages. Cliquez sur **Enable Logging** (Activer la journalisation) pour activer la journalisation si elle est désactivée.

La figure suivante montre les éléments du volet **Derniers messages Syslog ASDM**.

Illustration 5 : Derniers messages Syslog ASDM



Légende

Élément de GUI	Description
1	Faites glisser le **séparateur** vers le haut ou le bas pour redimensionner le volet.
2	Développe le volet. Cliquez sur l'icône **en forme de double-carré** pour rétablir la taille par défaut du volet.
3	Crée un volet flottant. Cliquez sur l'icône du **volet ancré** pour ancrer le volet.
4	Active ou désactive le masquage automatique. Lorsque le masquage automatique est activé, déplacez votre curseur sur le bouton **Derniers messages Syslog ASDM** dans le coin inférieur gauche et le volet s'affiche. Éloignez votre curseur du volet, et il disparaît.
5	Ferme le volet. Choisissez **Afficher les derniers messages Syslog ASDM** pour afficher le volet.
6	Cliquez sur l'icône **verte** sur le côté droit pour continuer à mettre à jour l'affichage des messages syslog.
7	Cliquez sur l'icône **rouge** à droite pour arrêter de mettre à jour l'affichage des messages syslog.
8	Cliquez sur l'icône **des filtres** sur le côté droit pour ouvrir le volet **Filtres de journalisation**.

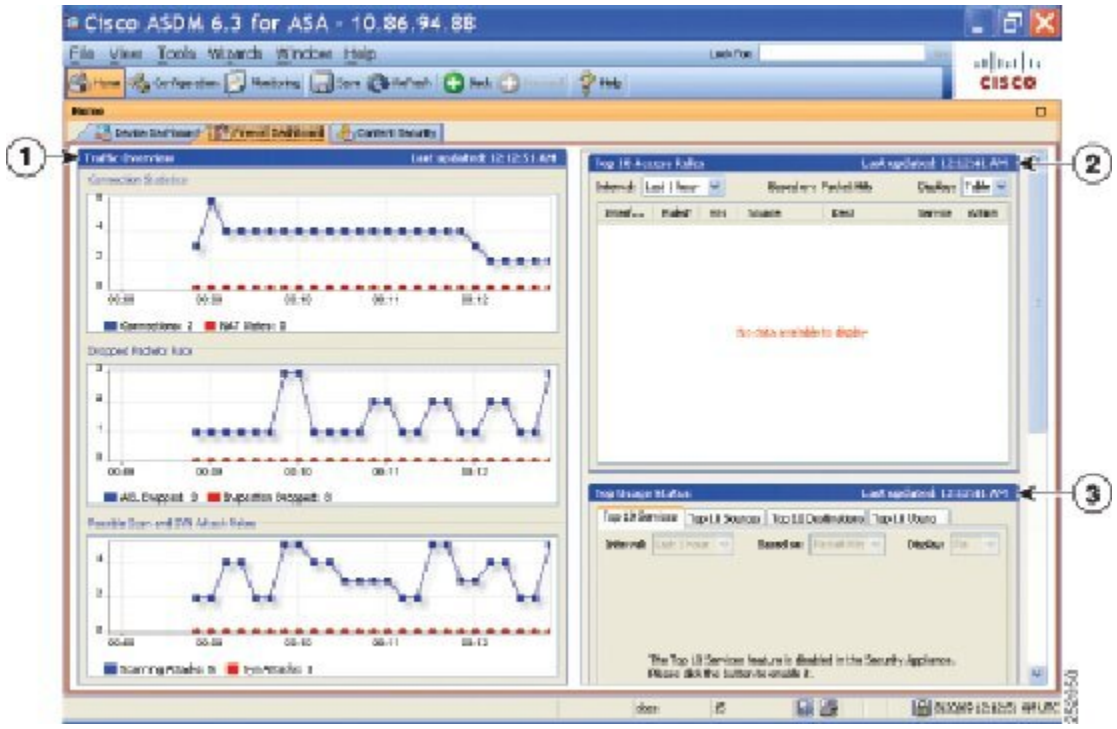
- Cliquez avec le bouton droit sur un événement et choisissez **Effacer le contenu** pour effacer les messages actuels.
- Effectuez un clic droit sur un événement et cliquez sur **Enregistrer le contenu** pour enregistrer les messages actuels dans un fichier sur votre PC.
- Cliquez avec le bouton droit sur un événement et choisissez **Copier** pour copier le contenu actuel.
- Cliquez avec le bouton droit sur un événement et choisissez **Paramètres de couleur** pour modifier les couleurs d'arrière-plan et de premier plan des messages syslog en fonction de leur gravité.

Onglet Tableau de bord du pare-feu

L'onglet **Firewall Dashboard** (Tableau de bord du pare-feu) vous permet d'afficher des informations importantes sur le trafic passant par votre ASA. Ce tableau de bord diffère selon que vous êtes en mode contexte unique ou en mode contexte multiple. En mode contexte multiple, le **Firewall Bodyboard** (Tableau de bord du pare-feu) est affiché dans chaque contexte.

La figure suivante montre certains des éléments de l'onglet **Firewall Dashboard** (Tableau de bord du pare-feu).

Illustration 6 : Onglet Tableau de bord du pare-feu



Légende

Élément de GUI	Description
1	Volet de présentation du trafic, à la page 77
2	Volet des 10 principales règles d'accès, à la page 77
3	Volet d'état de l'utilisation maximale, à la page 77
(non affiché)	Volet des dix principaux serveurs protégés sous attaque SYN, à la page 78
(non affiché)	Volet des 200 principaux hôtes, à la page 78
(non affiché)	Volet de résultats du filtre de trafic du réseau de zombies, à la page 78

Volet de présentation du trafic

Ce paramètre est activé par défaut. Si vous désactivez la détection de base des menaces (voir le guide de configuration de pare-feu), cette zone comprend un bouton **d'activation** qui vous permet d'activer la détection de base des menaces. Les statistiques d'exécution comprennent les renseignements suivants, qui sont *en affichage seulement* :

- Le nombre de connexions et les traductions NAT.
- Le taux de paquets abandonnés par seconde en raison des refus de liste d'accès et des inspections d'application.
- Le taux de paquets abandonnés par seconde qui sont identifiés comme faisant partie d'une attaque par analyse ou qui sont des sessions incomplètes détectées, comme l'attaque TCP SYN détectée ou l'attaque par une session UDP de données détectée.

Volet des 10 principales règles d'accès

Ce paramètre est activé par défaut. Si vous désactivez les statistiques de détection des menaces pour les règles d'accès (voir le guide de configuration du pare-feu), cette zone comprend un bouton **Enable** (Activer) qui vous permet d'activer les statistiques pour les règles d'accès.

Dans la vue Table (Tableau), vous pouvez sélectionner une règle dans la liste et cliquer avec le bouton droit sur la règle pour afficher l'élément de menu contextuel **Show Rule** (Afficher la règle). Choisissez cet élément pour accéder au tableau Access Rules (Règles d'accès) et sélectionnez cette règle dans ce tableau.

Volet d'état de l'utilisation maximale

L'option est désactivée par défaut. Ce volet comprend les quatre onglets suivants :

- **Top 10 Services** (10 principaux services) : service de détection des menaces
- **Top 10 Sources** (10 principales sources) — service de détection des menaces
- **Top 10 Destinations (10 principales destinations)** : service de détection des menaces
- **Top 10 Users (10 principaux utilisateurs)** : service de pare-feu d'identité

Les trois premiers onglets : **Top 10 Services** (10 principaux services), **Top 10 Sources** (10 principales sources) et **Top 10 Destinations** (10 principales destinations) fournissent des statistiques sur les services de détection des menaces. Chaque onglet comprend un bouton **Enable** (Activer) qui vous permet d'activer chaque service de détection des menaces. Vous pouvez les activer conformément au guide de configuration de pare-feu.

Le bouton **Enable (Activer) de l'onglet Top 10 Services (10 principaux services)** active les statistiques pour les ports et les protocoles (les deux doivent être activés pour l'affichage). Les boutons **Enable** (Activer) des onglets **Top 10 Sources (10 principales sources) et Top 10 Destinations (10 principales destinations)** activent les statistiques sur les hôtes. Les principales statistiques d'état d'utilisation des hôtes (sources et destinations), des ports et des protocoles sont affichées.

Le quatrième onglet, **Top 10 Users** (10 principaux utilisateurs), fournit des statistiques pour le service de pare-feu d'identité. Le service de pare-feu d'identité fournit un contrôle d'accès en fonction des identités des utilisateurs. Vous pouvez configurer des règles d'accès et des politiques de sécurité en fonction des noms d'utilisateur et du nom des groupes d'utilisateurs plutôt que d'utiliser les adresses IP sources. L'ASA fournit ce service en accédant à une base de données de mappage d'utilisateurs IP.

L'onglet **Top 10 Users** (10 principaux utilisateurs) affiche des données uniquement lorsque vous avez configuré l'une des fonctionnalités suivantes :

- La configuration du service de pare-feu d'identité, qui comprend la configuration de ces composants supplémentaires : Microsoft Active Directory et Cisco Active Directory (AD) Agent. Le service de pare-feu d'identité est activé à l'aide de la commande **user-identity enable** (activé par défaut) et de la commande **user-accounting statistics**.
- Configuration VPN utilisant un serveur RADIUS pour l'authentification, l'autorisation ou la comptabilité des utilisateurs VPN.

Selon l'option que vous choisissez, l'onglet **Top 10 Users** (10 principaux utilisateurs) affiche les statistiques sur les paquets EPS reçus, les paquets EPS envoyés et les attaques envoyées pour les 10 principaux utilisateurs. Pour chaque utilisateur (affiché comme *domaine\user_name*), l'onglet affiche le paquet EPE moyen, le paquet EPE actuel, le déclencheur et le nombre total d'événements pour cet utilisateur.

Mise en garde L'activation des statistiques peut affecter les performances de l'ASA, selon le type de statistiques activées. L'activation des statistiques sur l'hôte a une incidence importante sur les performances ; si vous avez une charge de trafic élevée, vous pouvez envisager d'activer temporairement ce type de statistiques. L'activation des statistiques pour les ports a cependant un effet faible.

Volet des dix principaux serveurs protégés sous attaque SYN

L'option est désactivée par défaut. Cette zone comprend un bouton **Enable** (Activer) qui vous permet d'activer la fonctionnalité ou vous pouvez l'activer conformément au guide de configuration du pare-feu. Les statistiques des dix principaux serveurs protégés par l'attaque sont affichées.

Pour le débit d'attaque moyen, l'ASA échantillonne les données toutes les 30 secondes pendant l'intervalle de débit (par défaut 30 minutes).

S'il y a plusieurs agresseurs, puis « <various> » s'affiche, suivi de la dernière adresse IP de l'agresseur.

Cliquez sur **Detail** (Détails) pour afficher les statistiques pour tous les serveurs (jusqu'à 1 000) au lieu de seulement 10 serveurs. Vous pouvez également afficher l'historique des données d'échantillonnage. L'ASA échantillonne le nombre d'attaques 60 fois au cours de l'intervalle de débit ; ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.

Volet des 200 principaux hôtes

L'option est désactivée par défaut. Affiche les 200 principaux hôtes connectés par l'intermédiaire de l'ASA. Chaque entrée d'un hôte contient l'adresse IP de l'hôte et le nombre de connexions initiées par l'hôte. Elle est mise à jour toutes les 120 secondes. Saisissez la commande **hpm topnenable** pour activer cet affichage.

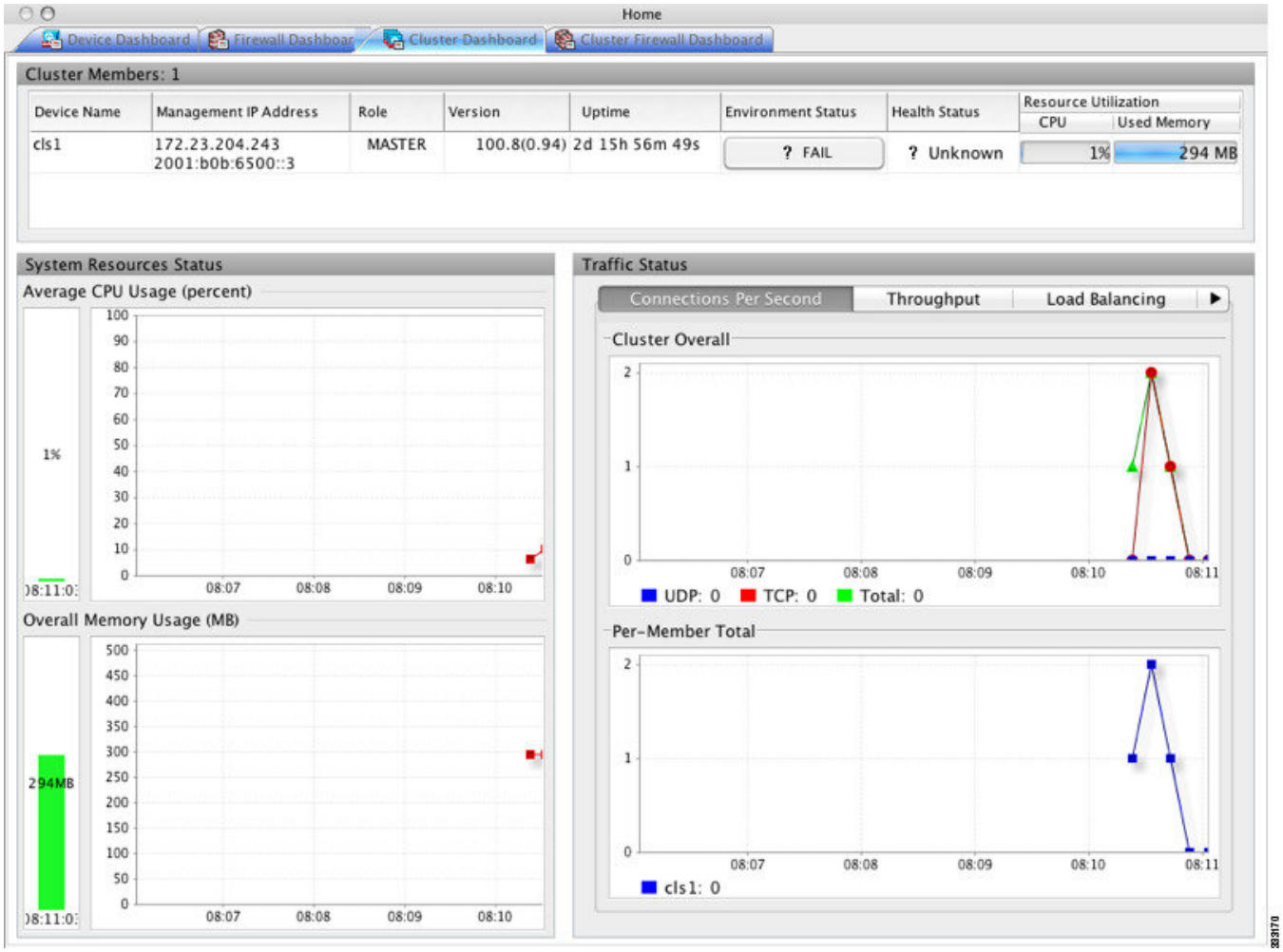
Volet de résultats du filtre de trafic du réseau de zombies

L'option est désactivée par défaut. Cette zone comprend des liens pour configurer le filtre de trafic de réseau de zombies. Les rapports sur les dix principaux sites de réseau de zombies, les ports et les hôtes infectés fournissent un instantané des données et peuvent ne pas correspondre aux dix principaux éléments depuis que les statistiques ont commencé à être collectées. Si vous cliquez avec le bouton droit sur une adresse IP, vous pouvez invoquer l'outil whois pour en savoir plus sur le site de réseau de zombies.

Consultez le guide de configuration du réseau de zombies pour en savoir plus.

Onglet Tableau de bord de la grappe

Lorsque vous activez la mise en grappe ASA et que vous êtes connecté à l'unité principale, l'onglet **Cluster Dashboard** (Tableau de bord de la grappe) affiche un résumé de l'appartenance à la grappe et de l'utilisation des ressources.



- **Cluster Members** (Membres de la grappe) : affiche les noms et les renseignements de base sur les membres qui composent la grappe (leur adresse IP de gestion, leur version, leur rôle dans la grappe, etc.) et leur état d'intégrité (état de l'environnement, état d'intégrité et utilisation des ressources).

Remarque En mode contexte multiple, si vous connectez ASDM au contexte admin, puis passez à un contexte différent, l'adresse IP de gestion répertoriée ne change pas pour afficher les adresses IP de gestion de contexte actuelles; elle continue d'afficher les adresses IP de gestion du contexte d'administration, y compris l'adresse IP de la grappe principale à laquelle ASDM est actuellement connecté.

- **System Resource Status** (État des ressources système) : affiche l'utilisation des ressources (CPU et mémoire) à l'échelle de la grappe et par périphérique, ainsi que les graphiques de trafic.
- **Traffic Status** (État du trafic) : chaque onglet comporte les graphiques suivants.
  - Onglet **Connections Per Second** (Connexions par seconde) :

    Cluster Overall (Ensemble de la grappe) : affiche le nombre de connexions par seconde dans l'ensemble de la grappe.

    Per-Member Total (Total par membre) : affiche le nombre moyen de connexions par seconde pour chaque membre.
  - Onglet **Throughput** (Débit) :

    Cluster Overall (Ensemble de la grappe) : affiche le débit de sortie agrégé dans l'ensemble de la grappe.

    Per-Member Throughput (Débit par membre) : affiche le débit de chaque membre, une ligne par membre.
  - Onglet **Load Balancing** (Équilibrage de charge) :

    Per-Member Percentage of Total Traffic (Pourcentage du trafic total par membre) : pour chaque membre, affiche le pourcentage du trafic total de la grappe que reçoit le membre.

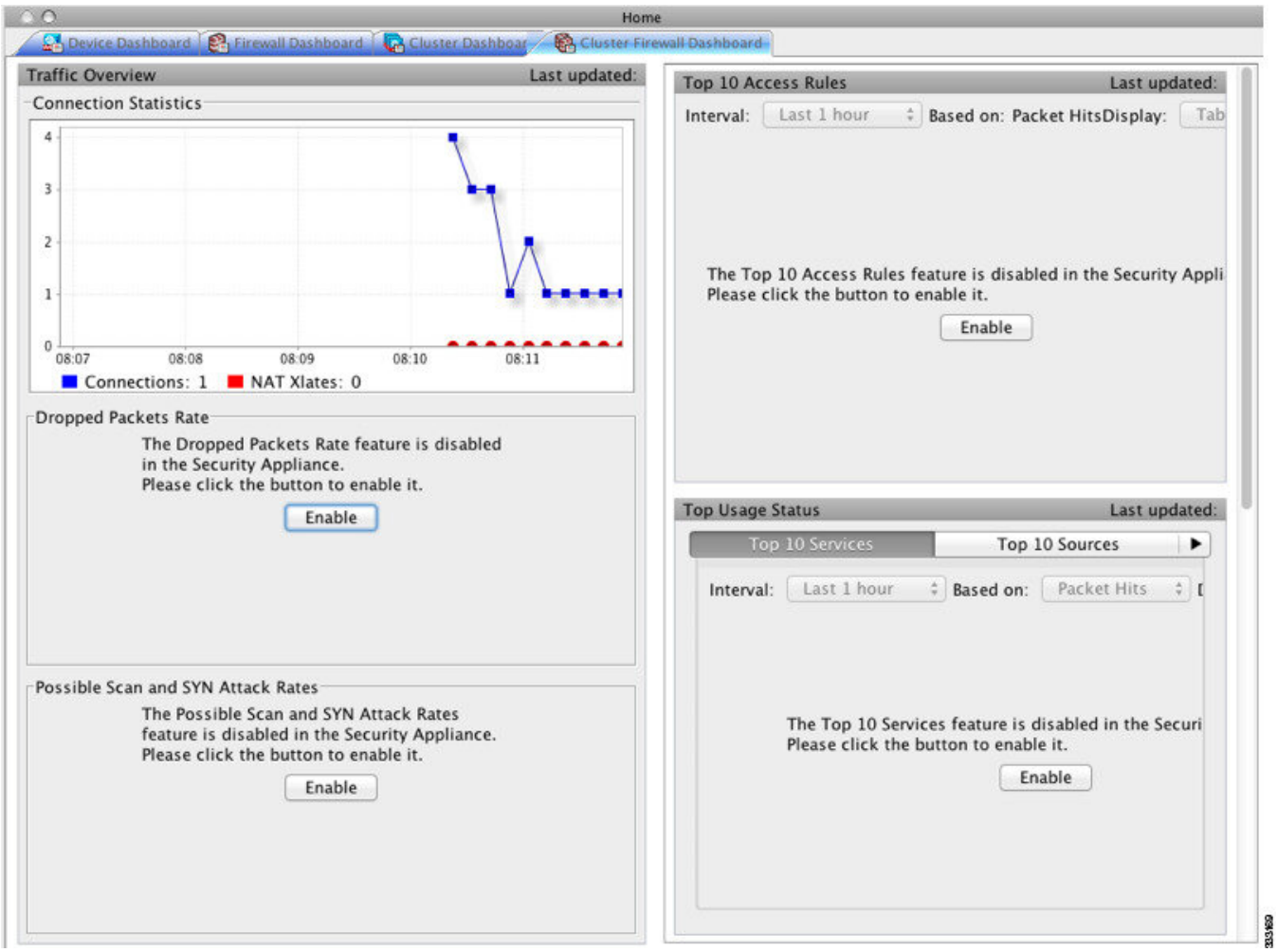
    Per-Member Locally Processed Traffic (Trafic traité localement par membre) : pour chaque membre, affiche le pourcentage du trafic traité localement.
  - Onglet **Control Link Usage** (Utilisation du lien de contrôle) :

    Per-Member Receival Capacity Utilization (Utilisation de la capacité de réception par membre) : pour chaque membre, affiche l'utilisation de la capacité de réception.

    Per-Member Transmittal Capacity Utilization (Utilisation de la capacité de transmission par membre) : pour chaque membre, affiche l'utilisation de la capacité de transmission.

Onglet Cluster Firewall Dashboard (Tableau de bord du pare-feu de grappe)

L'onglet **Cluster Firewall Dashboard** (Tableau de bord du pare-feu de grappe) affiche l'aperçu du trafic et les statistiques « top N », semblables à celles affichées dans **Firewall Dashboard** (Tableau de bord du pare-feu), mais agrégées sur l'ensemble de la grappe.



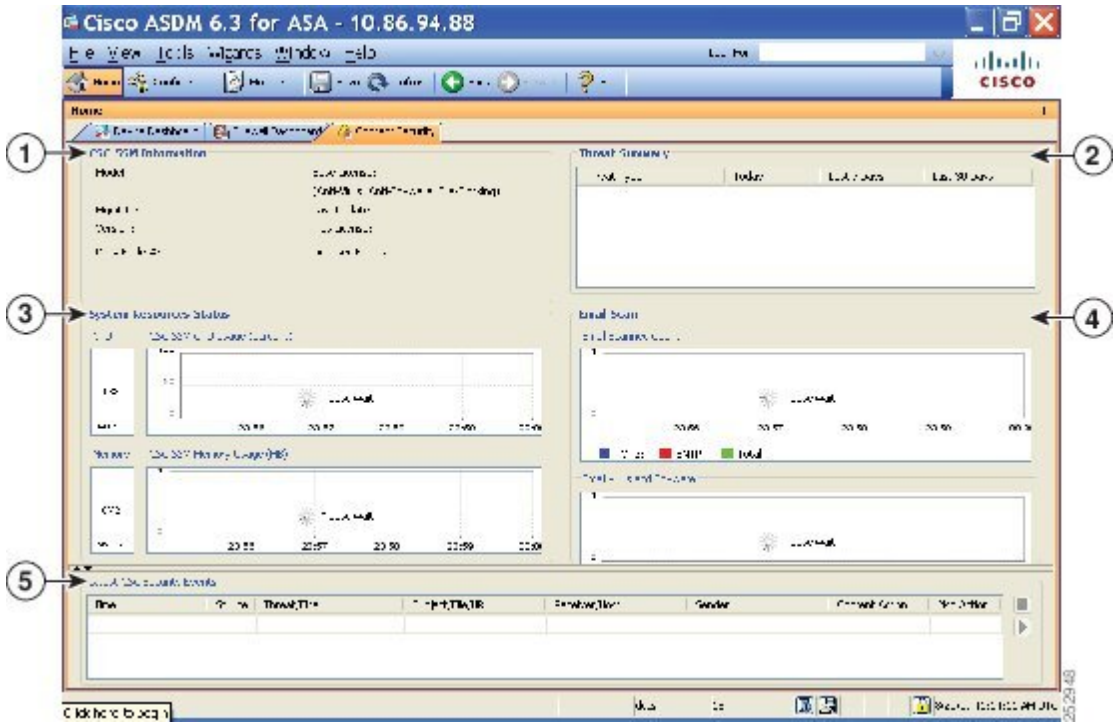
Onglet Content Security (Sécurité du contenu)

L'onglet **Content Security** (Sécurité du contenu) vous permet d'afficher des renseignements importants sur le SSM de sécurité et de contrôle du contenu (CSC). Ce volet s'affiche uniquement si le logiciel CSC exécuté sur le SSM CSC est installé dans l'appareil de sécurité adaptable Cisco.

Remarque Si vous n'avez pas terminé **l'assistant de configuration CSC** en choisissant **Configuration > Trend Micro Content Security (Sécurité du contenu Trend Micro) > CSC Setup (Configuration CSC)**, vous ne pouvez pas accéder aux volets sous **Home (Accueil) > Content Security (Sécurité du contenu)**. Au lieu de cela, une boîte de dialogue s'affiche et vous permet d'accéder à l'**assistant de configuration CSC** directement à partir de cet emplacement.

La figure suivante montre les éléments de l'onglet **Content Security** (Sécurité du contenu).

Illustration 7 : Onglet Content Security (Sécurité du contenu)



Légende

Élément de GUI	Description
1	Volet **CSC SSM Information** (Informations sur le SSM CSC).
2	Volet **Threat Summary** (Résumé des menaces). Affiche les données agrégées sur les menaces détectées par le SSM CSC, y compris les types de menaces suivants : virus, logiciels espions, URL filtrées ou bloquées, pourriel. Connexions bloquées, fichiers bloqués et services de contrôle des dommages.
3	**Volet System Resources Status** (État des ressources système).
4	**Volet Email Scan** (Analyse du courriel). Les graphiques affichent des données par intervalles de dix secondes.
5	Volet **Latest CSC Security Events** (Derniers événements de sécurité CSC).

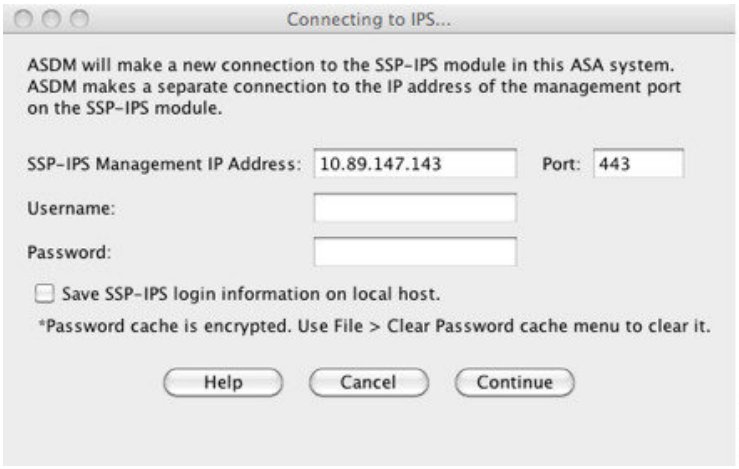
Onglet Intrusion Prevention (Prévention contre les intrusions)

L'onglet **Intrusion Prevention** (Prévention contre les intrusions) vous permet d'afficher des informations importantes sur IPS. Cet onglet s'affiche uniquement lorsqu'un module IPS est installé sur le périphérique de sécurité adaptable Cisco.

Pour vous connecter au module IPS, procédez comme suit :

1. Cliquez sur l'onglet **Intrusion Prevention** (Prévention contre les intrusions).

La boîte de dialogue **Connecting to IPS** (Connexion à l'IPS) s'affiche.

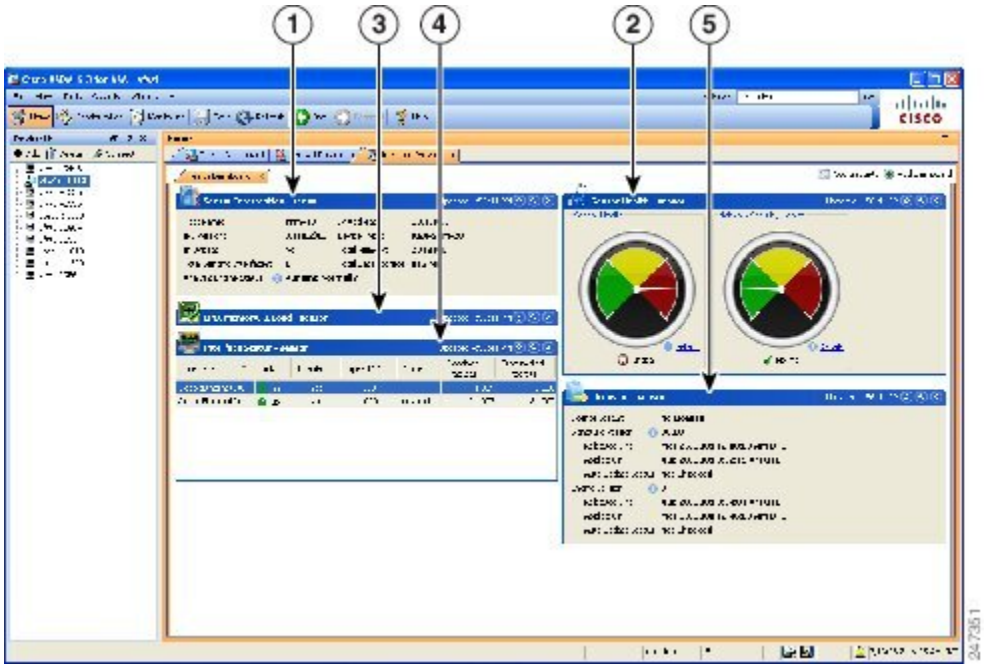


2. Saisissez l'adresse IP, le port, le nom d'utilisateur et le mot de passe. L'adresse IP et le port par défaut sont 192.168.1.2:443. Le nom d'utilisateur et le mot de passe par défaut sont **cisco** et **cisco**.
3. Cochez la case **Save IPS login information on local host** (Enregistrer les informations de connexion IPS sur l'hôte local) pour enregistrer les informations de connexion.
4. Cliquez sur **Continue** (Continuer).

Consultez le guide de démarrage rapide d'IPS pour obtenir plus d'informations sur la prévention des intrusions.

La figure suivante montre les éléments de l'onglet **Health Dashboard** (Tableau de bord d'intégrité), situé sous l'onglet **Intrusion Prevention** (Prévention contre les intrusions).

Illustration 8 : Onglet Intrusion Prevention (Prévention contre les intrusions) (Health Dashboard (Tableau de bord d'intégrité))

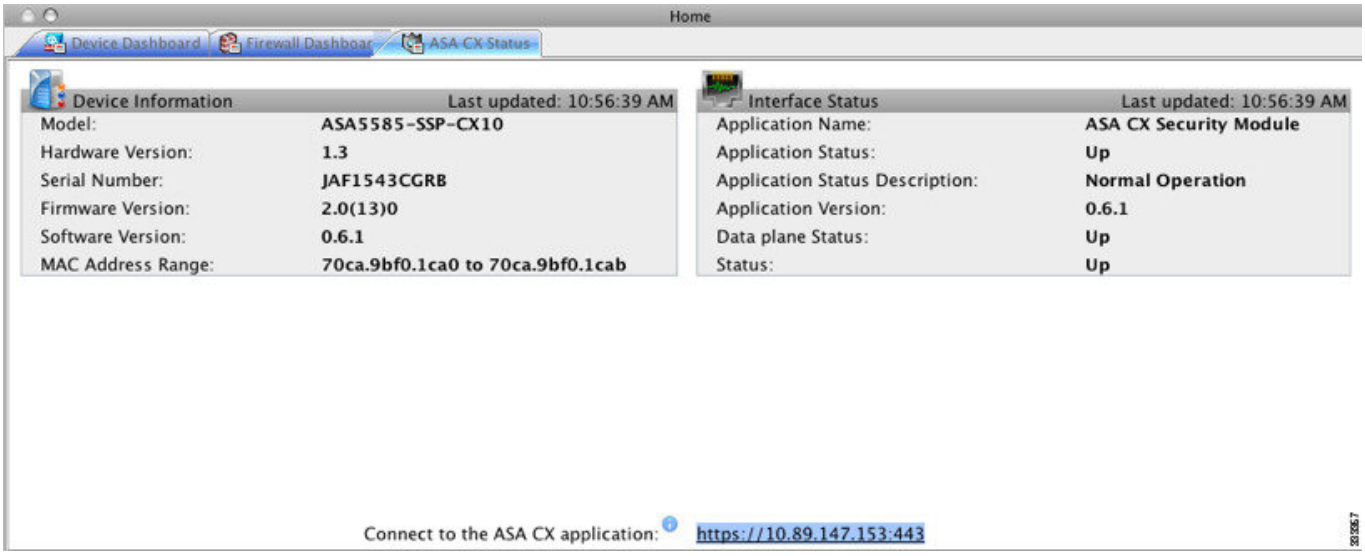


Légende

Élément de GUI	Description
1	Volet **Sensor Information** (Renseignements sur le capteur).
2	Volet **Sensor Health** (Intégrité du capteur).
3	Volet **CPU**, **Memory**, and **Load** (CPU, mémoire et charge).
4	Volet **Interface Status** (État de l'interface).
5	Volet **Licensing** (Gestion des licences).

Onglet ASA CX Status (État de l'ASA CX)

L'onglet **ASA CX Status** (État de l'ASA CX) vous permet d'afficher des informations importantes sur le module ASA CX. Cet onglet s'affiche uniquement lorsqu'un module ASA CX est installé sur l'ASA.



Onglets d'état ASA FirePower

L'onglet **ASA FirePOWER Status** (État de l'ASA FirePOWER) vous permet d'afficher les renseignements sur le module. Cela inclut les informations sur le module, telles que le modèle, le numéro de série, la version du logiciel, et l'état du module, comme le nom et l'état de l'application, l'état du plan de données et l'état général. Si le module est enregistré dans un centre de gestion FireSIGHT, vous pouvez cliquer sur le lien pour ouvrir l'application et effectuer une analyse plus approfondie et la configuration du module.

Cet onglet s'affiche uniquement si un module ASA FirePOWER est installé dans le périphérique.

Si vous gérez le module ASA FirePOWER avec ASDM plutôt que FireSIGHT Management Center, il existe des onglets supplémentaires :

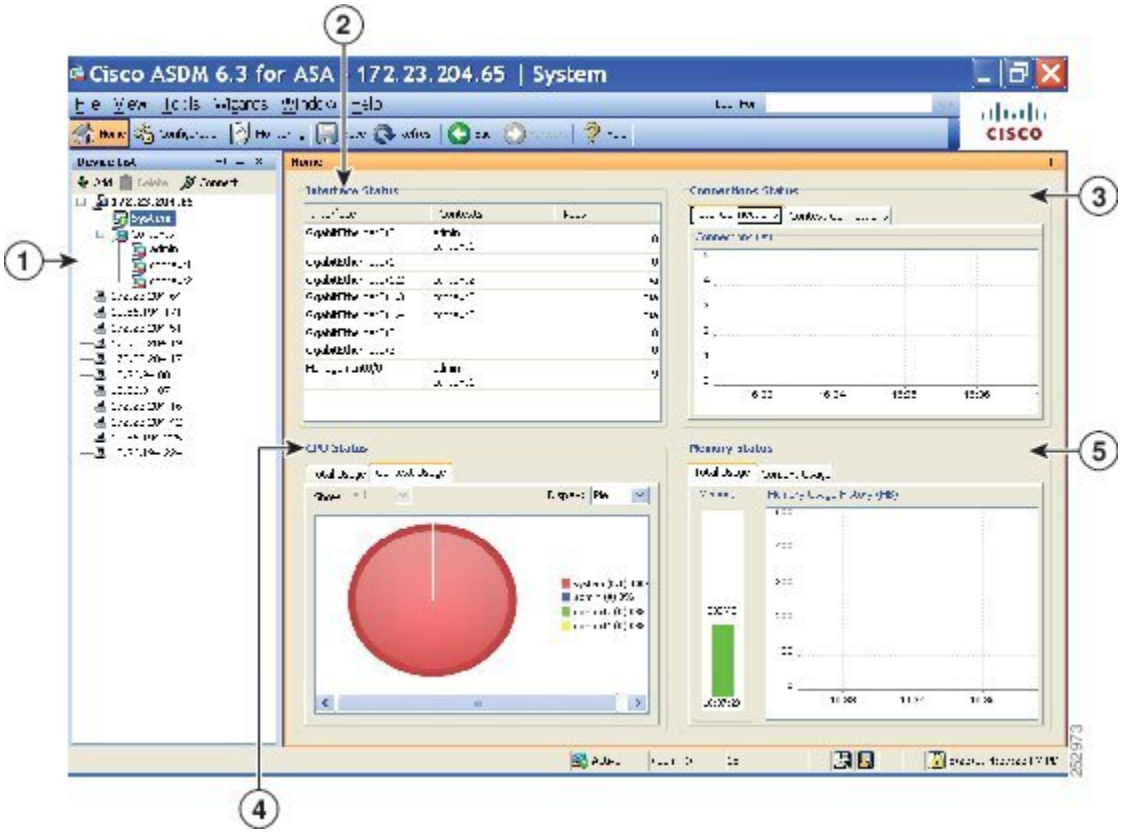
- **ASA FirePOWER Dashboard** (Tableau de bord ASA FirePOWER) : le tableau de bord fournit des informations récapitulatives sur le logiciel exécuté sur le module, les mises à jour de produits, les licences, la charge du système, l'utilisation du disque, l'heure du système et l'état des interfaces.
- **ASA FirePOWER Reporting** (Rapports ASA FirePOWER) : la page de rapports fournit les 10 principaux tableaux de bord pour une grande variété de statistiques du module, telles que les catégories Web, les utilisateurs, les sources et les destinations du trafic passant par le module.

Volet d'accueil (système)

Le volet **Home** (Accueil) du système ASDM vous permet d'afficher des informations d'état importantes sur votre appareil de sécurité adaptable Cisco. Plusieurs des détails disponibles dans le volet **Home** (Accueil) du système ASDM sont disponibles ailleurs dans ASDM, mais ce volet montre en un coup d'œil comment votre ASA fonctionne. Les informations sur l'état dans le volet **Home** (Accueil) du système sont mises à jour toutes les dix secondes.

La figure suivante montre les éléments du volet **Home** (Accueil) du système.

Illustration 9 : Panneau d'accueil du système



Légende

Élément d'interface graphique	Description
1	Sélection du système ou du contexte.
2	Volet **Interface Status** (État de l'interface). Choisissez une interface pour afficher la quantité totale de trafic via l'interface.
3	Volet **Connection Status** (État de la connexion).
4	Volet **CPU Status** (État du processeur).
5	Volet **Memory Status** (État de la mémoire).

Définir les préférences ASDM

Vous pouvez définir le comportement de certains paramètres ASDM.

Pour modifier les paramètres des messages du journal système, procédez comme suit :

Procédure

Étape 1 Choisissez **Tools (Outils)** > **Preferences (Préférences)**.

La boîte de dialogue **Preferences** (Préférences) apparaît, avec trois onglets : **General** (Général), **Rules Table** (Tableau de règles) et **Syslog**.

Étape 2 Pour définir vos paramètres, cliquez sur l'un de ces onglets : l'onglet **General** (Général) pour préciser les préférences générales; l'onglet **Rules Table** (Tableau de règles) pour préciser les préférences du tableau de règles; et l'onglet **Syslog** pour préciser l'apparence des messages de journal système affichés dans le volet **Home** (Accueil) et pour activer l'affichage d'un message d'avertissement pour les messages de journal système liés à NetFlow.

Étape 3 Dans l'onglet **General** (Général), configurez les éléments suivants :

- Cochez la case **Warn that configuration in ASDM is out of sync with the configuration in ASA** (Avertissement que la configuration dans ASDM n'est pas synchronisée avec la configuration dans ASA) pour recevoir une notification lorsque la configuration de démarrage et la configuration en cours d'exécution ne sont plus synchronisées l'une avec l'autre.
- Cochez la case **Show configuration restriction message to read-only user** (Afficher la restriction de configuration pour l'utilisateur en lecture seule) pour afficher le message suivant à l'intention d'un utilisateur en lecture seule au démarrage. Cette option est cochée par défaut.

```
"You are not allowed to modify the ASA configuration,
because you do not have sufficient privileges."
```

- Cochez la case **Show configuration restriction message on a slave unit in an ASA cluster** (Afficher le message de restriction de configuration sur une unité esclave dans une grappe ASA) pour afficher un message de restriction de configuration à l'intention d'un utilisateur connecté à une unité esclave.
- Cochez la case **Confirm before exiting ASDM** (Confirmer avant de quitter ASDM) pour afficher une invite lorsque vous tentez de fermer ASDM afin de confirmer que vous souhaitez quitter. Cette option est cochée par défaut.
- Cochez la case **Enable screen reader support (requires ASDM restart)** (Activer la prise en charge des lecteurs d'écran [nécessite le redémarrage d'ASDM]) pour permettre aux lecteurs d'écran de fonctionner. Vous devez redémarrer ASDM pour activer cette option.
- Cochez la case **Warn of insufficient ASA memory when ASDM loads** (Avertissement de mémoire ASA insuffisante lors du chargement d'ASDM) pour recevoir une notification lorsque la quantité minimale de mémoire ASA est insuffisante pour exécuter toutes les fonctionnalités de l'application ASDM. ASDM affiche l'avertissement de mémoire dans un message de bannière de texte au démarrage, affiche un message dans le texte de la barre de titre dans ASDM et envoie une alerte de journal système une fois toutes les 24 heures.
- Dans la zone **Communications** :
  - Cochez la case **Preview commands before sending them to the device** (Aperçu des commandes avant de les envoyer au périphérique) pour afficher les commandes CLI générées par ASDM.
  - Cochez la case **Enable cumulative (batch) CLI delivery** (Activer l'envoi cumulatif [par lots] des commandes CLI) pour envoyer plusieurs commandes dans un seul groupe à l'ASA.
  - Dans le champ **Minimum Configuration Sending Timeout** (Délai minimal d'envoi de la configuration), saisissez le délai minimal en secondes avant l'affichage d'un message de délai d'expiration lors de l'envoi d'une configuration. La valeur par défaut est de 60 secondes.
  - Pour le système en mode de contexte multiple, dans le champ **Graph User time interval in System Context** (Intervalle utilisateur des graphiques dans le contexte système), saisissez le délai entre les mises à jour des graphiques dans le volet Home (Accueil), entre 1 et 40 secondes. La valeur par défaut est de 10 secondes.
- Dans la zone **Logging** (Journalisation) :
  - Cochez la case **Enable logging to the ASDM Java console** (Activer la journalisation dans la console Java ASDM) pour configurer la journalisation Java.
  - Choisissez le niveau de gravité dans la liste déroulante **Logging Level** (Niveau de journalisation).
- Dans la zone **Packet Capture Wizard** (Assistant de capture de paquets), pour afficher les paquets capturés, saisissez le nom de l'application **Network Sniffer Application** (Application d'analyse réseau) ou cliquez sur **Browse** (Parcourir) pour la trouver dans le système de fichiers.
- Dans la zone **SFR Location Wizard** (Assistant d'emplacement SFR), spécifiez l'emplacement d'installation des fichiers de gestion locaux du module ASA FirePOWER. Vous devez avoir des privilèges de lecture/écriture à l'emplacement configuré.

Étape 4 Sous l'onglet **Rules Table** (Tableau de règles), spécifiez les éléments suivants :

- Les paramètres d'affichage vous permettent de modifier la façon dont les règles s'affichent dans le tableau des règles.

- Cochez la case **Auto-expand network and service object groups with specified prefix** (Développer automatiquement les groupes d'objets réseau et de service avec le préfixe spécifié) pour afficher automatiquement les groupes d'objets réseau et de service développés en fonction du paramètre Auto-Expand Prefix (Préfixe de développement automatique).
- Saisissez le préfixe des groupes d'objets réseau et de service à développer automatiquement lorsqu'il est affiché dans le champ **Auto-Expand Prefix** (Préfixe de développement automatique).
- Cochez la case **Show members of network and service object groups** (Afficher les membres des groupes d'objets réseau et de service) pour afficher les membres des groupes d'objets réseau et de service ainsi que le nom du groupe dans le tableau des règles. Si la case n'est pas cochée, seul le nom du groupe s'affiche.
- Saisissez le nombre de groupes d'objets réseau et de service à afficher dans le champ **Limit Members To** (Limiter le nombre de membres à). Lorsque les membres du groupe d'objets sont affichés, seuls les *n* premiers membres sont affichés.
- Cochez la case **Show all actions for service policy rules** (Afficher toutes les actions des règles de stratégie de service) pour afficher toutes les actions dans le tableau des règles. Lorsque cette option n'est pas cochée, un résumé s'affiche.

- Les paramètres de déploiement vous permettent de configurer le comportement de l'ASA lors du déploiement de modifications du tableau des règles.
  - Cochez la case **Issue "clear xlate" command when deploying access lists** (Exécuter la commande « clear xlate » lors du déploiement des listes d'accès) pour effacer la table NAT lors du déploiement de nouvelles listes d'accès. Ce paramètre garantit que les listes d'accès configurées sur l'ASA sont appliquées à toutes les adresses traduites.

- Les paramètres du nombre de résultats des règles d'accès vous permettent de configurer la fréquence à laquelle le nombre de résultats est mis à jour dans le tableau des règles d'accès. Le nombre de résultats s'applique uniquement aux règles explicites. Aucun nombre de résultats ne s'affichera pour les règles implicites dans le tableau des règles d'accès.
  - Cochez la case **Update access rule hit counts automatically** (Mettre à jour automatiquement le nombre de correspondances des règles d'accès) pour que le nombre de correspondances soit automatiquement mis à jour dans le tableau des règles d'accès.
  - Précisez la fréquence en secondes à laquelle la colonne du nombre de résultats est mise à jour dans le tableau des règles d'accès. Les valeurs valides vont de 10 à 86 400 secondes.

Étape 5 Sous l'onglet **Syslog**, spécifiez les éléments suivants :

- Dans la zone **Syslog Colors** (Couleurs du journal système), vous pouvez personnaliser l'affichage des messages en configurant les couleurs d'arrière-plan ou de premier plan pour les messages à chaque niveau de gravité. La colonne **Severity** (Gravité) répertorie chaque niveau de gravité par nom et par numéro. Pour modifier la couleur d'arrière-plan ou de premier plan des messages à un niveau de gravité spécifié, cliquez sur la colonne correspondante. La boîte de dialogue **Pick a Color** (Choisir une couleur) s'affiche. Cliquez sur l'un des onglets suivants :
  - Choisissez une couleur dans la palette sous l'onglet **Swatches** (Nuances), puis cliquez sur **OK**.
  - Précisez les paramètres H, S et B sous l'onglet **HSB**, puis cliquez sur **OK**.
  - Précisez les paramètres de rouge, vert et bleu sous l'onglet **RVB**, puis cliquez sur **OK**.

- Cochez la case **Warn to disable redundant syslog messages when NetFlow action is first applied to the global service policy rule** (Avertir pour désactiver les messages syslog redondants lorsque l'action NetFlow est appliquée pour la première fois à la règle de stratégie de service globale) dans la zone **NetFlow** pour activer l'affichage d'un message d'avertissement invitant à désactiver les messages syslog redondants.

Étape 6 Après avoir spécifié les paramètres sur ces trois onglets, cliquez sur **OK** pour enregistrer vos paramètres et fermer la boîte de dialogue **Preferences** (Préférences).



Remarque Chaque fois que vous cochez ou décochez un paramètre de préférences, la modification est enregistrée dans le fichier .conf et devient disponible pour toutes les autres sessions ASDM en cours d'exécution sur le poste de travail à ce moment-là. Vous devez redémarrer ASDM pour que tous les changements prennent effet.

Rechercher avec l'assistant ASDM

L'outil ASDM Assistant vous permet de rechercher et d'afficher l'aide procédurale d'ASDM utile concernant certaines tâches.

Choisissez **View (Afficher)** > **ASDM Assistant (Assistant ASDM)** > **How Do I? (Comment faire?)** pour accéder aux informations, ou saisissez une demande de recherche dans le champ **Look For** (Rechercher) de la barre de menus. Choisissez **How Do I?** (Comment faire?) Dans la liste déroulante **Find** (Rechercher) pour commencer la recherche.

Pour afficher l'assistant ASDM, procédez comme suit :

Procédure

Étape 1 Choisissez **View (Afficher)** > **ASDM Assistant (Assistant ASDM)**.

Le volet **ASDM Assistant** (Assistant ASDM) apparaît.

Étape 2 Saisissez les informations que vous souhaitez trouver dans le champ **Search** (Rechercher), puis cliquez sur **Go** (Aller).

Les informations demandées s'affichent dans le volet **Search Results** (Résultats de la recherche).

Étape 3 Cliquez sur les liens qui apparaissent dans les sections **Search Results (Résultats de la recherche) et Features (Fonctionnalités)** pour obtenir plus de détails.

Activation des mesures d'historique

Le volet History Metrics (Mesures d'historique) vous permet de configurer l'ASA pour conserver un historique des statistiques. Si vous n'activez pas les mesures d'historique, vous pouvez uniquement superviser les

statistiques en temps réel. L'activation des mesures d'historique vous permet d'afficher les graphiques de statistiques des 10 dernières minutes, 60 minutes, 12 heures et 5 jours.

Pour configurer les mesures d'historique, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **History Metrics (Mesures d'historique)**.

Le volet **History Metrics** (Mesures d'historique) apparaît.

Étape 2 Cochez la case **ASDM History Metrics** (Mesures d'historique ASDM) pour activer les mesures d'historique, puis cliquez sur **Apply** (Appliquer).

Commandes non prises en charge

ASDM prend en charge presque toutes les commandes disponibles pour l'ASA, mais ASDM ignore certaines commandes dans une configuration existante. La plupart de ces commandes peuvent rester dans votre configuration; consultez **Tools (Outils) > Show Commands Ignored by ASDM on Device (Afficher les commandes ignorées par ASDM sur le périphérique)** pour de plus amples renseignements.

Commandes ignorées et d'affichage uniquement

Le tableau suivant répertorie les commandes prises en charge par ASDM dans la configuration lorsqu'elles sont ajoutées par l'intermédiaire de l'interface de ligne de commande, mais qui ne peuvent pas être ajoutées ou modifiées dans ASDM. Si ASDM ignore la commande, elle ne s'affiche pas du tout dans l'interface graphique d'ASDM. Si la commande est en affichage uniquement, elle s'affiche dans l'interface graphique, mais vous ne pouvez pas la modifier.

Tableau 6 : Commandes non prises en charge

Commandes non prises en charge	Comportement ASDM
capture	Ignoré.
coredump	Ignoré. Cela ne peut être configuré qu'à l'aide de l'interface de ligne de commande.
crypto engine large-mod-accel	Ignoré.
dhcp-server (tunnel-group name general-attributes)	ASDM n'autorise qu'un seul paramètre pour tous les serveurs DHCP.
eject	Non pris en charge.
established	Ignoré.
failover timeout	Ignoré.

Commandes non prises en charge	Comportement ASDM
fips	Ignoré.
nat-assigned-to-public-ip	Ignoré.
pager	Ignoré.
pim accept-register route-map	Ignoré. Vous pouvez configurer uniquement l'option **list** à l'aide d'ASDM.

service-policy global	Ignoré s'il utilise une classe **match access-list**. Par exemple :
	
	`access-list myacl extended permit ip any any`
	`class-map mycm`
	`  match access-list myacl`
	`policy-map mypm`
	`  class mycm`
	`    inspect ftp`
	`service-policy mypm global`

set metric	Ignoré.
sysopt nodnsalias	Ignoré.
sysopt uauth allow-http-cache	Ignoré.
terminal	Ignoré.
threat-detection rate	Ignoré.

Effets des commandes non prises en charge

Si ASDM charge une configuration en cours d'exécution existante et trouve d'autres commandes non prises en charge, le fonctionnement d'ASDM n'est pas affecté. Choisissez **Tools (Outils) > Show Commands Ignored by ASDM on Device (Afficher les commandes ignorées par ASDM sur le périphérique)** pour afficher les commandes non prises en charge.

Masques de sous-réseau discontinus non pris en charge

ASDM ne prend pas en charge les masques de sous-réseau discontinus tels que 255.255.0.255. Par exemple, vous ne pouvez pas utiliser les éléments suivants :

```
ip address inside 192.168.2.1 255.255.0.255
```

Commandes utilisateur interactives non prises en charge par l'outil CLI ASDM

L'outil CLI ASDM ne prend pas en charge les commandes utilisateur interactives. Si vous saisissez une commande CLI qui nécessite une confirmation interactive, ASDM vous invite à saisir « [yes/no] » mais ne reconnaît pas votre entrée. ASDM expire ensuite en attendant votre réponse.

Par exemple :

1. Choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.
2. Entrez la commande **crypto key generate rsa**.

   ASDM génère la clé RSA de 1 024 bits par défaut.
3. Entrez à nouveau la commande **crypto key generate rsa**.

   Au lieu de régénérer les clés RSA en remplaçant la clé précédente, ASDM affiche l'erreur suivante :

```
Do you really want to replace them? [yes/no]:WARNING: You already have
RSA ke0000000000000$A key
Input line must be less than 16 characters in length.

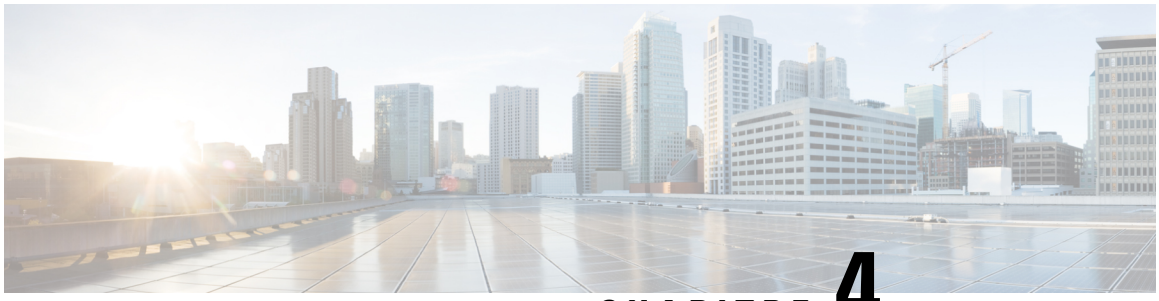
%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:

%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

Solution de rechange:

- Vous pouvez configurer la plupart des commandes qui nécessitent l'intervention de l'utilisateur au moyen des volets ASDM.
- Pour les commandes CLI qui ont une option **noconfirm**, utilisez cette option lors de la saisie de la commande CLI. Par exemple :

```
crypto key generate rsa noconfirm
```



CHAPITRE 4

Licences : licence à clé d'autorisation de produit pour l'ISA 3000

Une licence spécifie les options qui sont activées sur un ASA donné. Ce document décrit les licences de clé d'autorisation de produit (PAK) pour l'ISA 3000. Pour d'autres modèles, consultez Licences : gestion des licences logicielles Smart, à la page 125.

- À propos des licences PAK, à la page 93
- Lignes directrices relatives aux licences PAK, à la page 101
- Configurer les licences PAK, à la page 103
- Configurer une licence partagée (Secure Client (services client sécurisés) 3 et versions antérieures), à la page 108
- Licences de fonctionnalités prises en charge par modèle, à la page 113
- Supervision des licences PAK, à la page 115
- Historique des licences PAK, à la page 116

À propos des licences PAK

Une licence spécifie les options qui sont activées sur un ASA donné. Elle est représentée par une clé d'activation qui est une valeur de 160 bits (5 mots de 32 bits ou 20 octets). Cette valeur encode le numéro de série (une chaîne de 11 caractères) et les fonctionnalités activées.

Licence préinstallée

Par défaut, votre ASA est livré avec une licence déjà installée. Cette licence peut être la licence de base, à laquelle vous souhaitez ajouter d'autres licences, ou toutes vos licences peuvent déjà être installées, selon ce que vous avez commandé et ce que votre prestataire a installé pour vous.

Sujets connexes

Supervision des licences PAK, à la page 115

Licence permanente

Vous pouvez installer une clé d'activation permanente. La clé d'activation permanente comprend toutes les fonctionnalités sous licence en une seule clé. Si vous installez également des licences à durée limitée, l'ASA combine les licences permanentes et à durée limitée en une licence en cours d'exécution.

Sujets connexes

Association des licences permanentes et à durée limitée, à la page 94

Licences à durée limitée

En plus des licences permanentes, vous pouvez acheter des licences à durée limitée ou recevoir une licence d'évaluation d'une durée limitée. Par exemple, vous pouvez acheter une licence Secure Client (services client sécurisés) Premium à durée limitée pour gérer les pics à court terme du nombre d'utilisateurs SSL VPN simultanés.

Lignes directrices relatives à l'activation de la licence à durée limitée

- Vous pouvez installer plusieurs licences à durée limitée, y compris plusieurs licences pour la même fonctionnalité. Cependant, une seule licence à durée limitée par fonctionnalité peut être *active* à la fois. La licence inactive reste installée et prête à l'emploi. Par exemple, si vous installez une licence Secure Client (services client sécurisés) Premium de 1 000 sessions et une licence Secure Client (services client sécurisés) Premium de 2 500 sessions, une seule de ces licences peut être active.
- Si vous activez une licence d'évaluation qui comporte plusieurs fonctionnalités dans la clé, vous ne pouvez pas activer une autre licence à durée limitée pour l'une des fonctionnalités incluses.

Fonctionnement de la minuterie des licences à durée limitée

- La minuterie des licences à durée limitée commence le compte à rebours lorsque vous l'activez sur l'ASA.
- Si vous cessez d'utiliser la licence à durée limitée avant son expiration, la minuterie s'arrête. La minuterie ne redémarre que lorsque vous réactivez la licence à durée limitée.
- Si la licence à durée limitée est active et que vous arrêtez l'ASA, la minuterie cesse le compte à rebours. La licence à durée limitée ne commence à compter que lorsque l'ASA est en cours d'exécution. Le paramètre de l'horloge système n'a pas d'incidence sur la licence; seul le temps de disponibilité de l'ASA est pris en compte dans la durée de la licence.

Association des licences permanentes et à durée limitée

Lorsque vous activez une licence à durée limitée, les fonctionnalités des licences permanentes et à durée limitée se combinent pour former la licence d'exécution. La façon dont les licences permanentes et à durée limitée se combinent dépend du type de licence. Le tableau suivant répertorie les règles de combinaison pour chaque licence de fonctionnalité.

Remarque Même lorsque la licence permanente est utilisée, si la licence à durée limitée est active, son compte continue.

Tableau 7 : Règles de combinaison de licences à durée limitée

Fonctionnalité à durée limitée	Règle de licence combinée
Sessions Premium Secure Client (services client sécurisés)	La valeur la plus élevée est utilisée, qu'elle soit à durée limitée ou permanente. Par exemple, si la licence permanente est de 1 000 sessions et que la licence à durée limitée est de 2 500 sessions, les 2 500 sessions sont activées. Généralement, vous n'installerez pas une licence à durée limitée ayant une capacité inférieure à la licence permanente, mais si vous le faites, la licence permanente est utilisée.
Sessions de mandataire pour les communications unifiées	Les sessions de licences à durée limitée sont ajoutées aux sessions permanentes, jusqu'à la limite de plateformes. Par exemple, si la licence permanente est de 2 500 sessions et que la licence à durée limitée est de 1 000 sessions, 3 500 sessions sont activées tant que la licence à durée limitée est active.
Tous les autres	La valeur la plus élevée est utilisée, qu'elle soit à durée limitée ou permanente. Pour les licences dont l'état est activé ou désactivé, la licence ayant l'état activé est utilisée. Pour les licences à niveaux numériques, la valeur la plus élevée est utilisée. Généralement, vous n'installerez pas une licence à durée limitée ayant une capacité inférieure à la licence permanente, mais si vous le faites, la licence permanente est utilisée.

Sujets connexes

Supervision des licences PAK, à la page 115

Empilage des licences à durée limitée

Dans de nombreux cas, vous devrez peut-être renouveler votre licence temporaire et effectuer une transition transparente de l'ancienne licence à la nouvelle. Pour les fonctionnalités qui ne sont disponibles qu'avec une licence à durée limitée, il est particulièrement important que la licence n'expire pas avant que vous puissiez appliquer la nouvelle licence. L'ASA vous permet d'*empiler* des licences à durée limitée afin que vous n'ayez pas à vous soucier de l'expiration de la licence ou de la perte de temps sur vos licences en raison de l'installation de la nouvelle licence plus tôt.

Lorsque vous installez une licence à durée limitée identique à celle déjà installée, les licences sont combinées et la durée est égale à la durée combinée.

Par exemple :

1. Vous installez une licence Secure Client (services client sécurisés) Premium de 8 semaines de 1 000 sessions et l'utilisez pendant 2 semaines (il reste 6 semaines).
2. Vous installez ensuite une autre licence de 8 semaines de 1 000 sessions, et les licences se combinent pour offrir 1 000 sessions pendant 14 semaines (8 semaines plus 6 semaines).

Si les licences ne sont pas identiques (par exemple, une licence Secure Client (services client sécurisés) Premium de 1 000 sessions et une licence de 2 500 sessions), elles ne sont *pas* combinées. Comme une seule licence à durée limitée par fonctionnalité peut être active, une seule des licences peut être active.

Bien que les licences non identiques ne se combinent pas, lorsque la licence actuelle expire, l'ASA active automatiquement une licence installée de la même fonctionnalité, si elle est disponible.

Sujets connexes

Activer ou désactiver les clés, à la page 107
Échéance de la licence à durée limitée, à la page 96

Échéance de la licence à durée limitée

Lorsque la licence actuelle d'une fonctionnalité expire, l'ASA active automatiquement une licence installée de la même fonctionnalité, si elle est disponible. Si aucune autre licence à durée limitée n'est disponible pour cette fonctionnalité, la licence permanente est utilisée.

Si vous avez plusieurs licences supplémentaires à durée limitée installées pour une fonctionnalité, l'ASA utilise la première licence qu'il trouve; la licence utilisée n'est pas configurable par l'utilisateur et dépend des opérations internes. Si vous préférez utiliser une licence autre que celle activée par l'ASA, vous devez activer manuellement la licence de votre choix.

Par exemple, vous disposez d'une licence Secure Client (services client sécurisés) Premium à durée limitée de 2 500 sessions (active), d'une licence Secure Client (services client sécurisés) Premium à durée limitée de 1 000 sessions (inactive) et d'une licence permanente Secure Client (services client sécurisés) Premium de 500 sessions. Lorsque la licence de 2 500 sessions expire, l'ASA active la licence de 1 000 sessions. Après l'expiration de la licence de 1 000 sessions, l'ASA utilise la licence permanente de 500 sessions.

Sujets connexes

Activer ou désactiver les clés, à la page 107

Remarques relatives à la licence

Les sections suivantes contiennent des renseignements supplémentaires sur les licences.

LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement

La licence Secure Client Advantage ou Premier est une licence multi-utilisation que vous pouvez appliquer à plusieurs ASA, qui partagent tous un ensemble d'utilisateurs comme spécifié par la licence. La licence VPN client sécurisé uniquement s'applique à un ASA spécifique. Consultez https://www.cisco.com/go/license et attribuez la clé PAK séparément à chaque ASA. Lorsque vous appliquez la clé d'activation résultante à un ASA, elle active les fonctionnalités VPN au maximum autorisé, mais le nombre réel d'utilisateurs uniques pour tous les ASA partageant la licence ne doit pas dépasser la limite de licence. Pour obtenir plus de renseignements, consultez la section :

- Guide de commande Cisco Secure Client (services client sécurisés)
- Foire aux questions (FAQ) Secure Client (services client sécurisés) Licensing

Remarque La licence Secure Client Premier est la seule licence Secure Client Premier prise en charge pour le mode de contexte multiple. De plus, en mode de contexte multiple, cette licence doit être appliquée à chaque unité d'une paire de basculement; la licence n'est pas agrégée.

Autre licence VPN

Les autres homologues VPN comprennent les types de VPN suivants :

- VPN d'accès à distance IPsec avec IKEv1
- VPN de site à site IPsec avec IKEv1
- VPN de site à site IPsec avec IKEv2

Cette licence est incluse dans la licence de base.

Nombre total de sessions VPN combinées, tous types

- Le nombre total d'homologues VPN est le nombre maximum d'homologues VPN autorisés pour les homologues Secure Client (services client sécurisés) et autres homologues VPN combinés. Par exemple, si le total est de 1 000, vous pouvez autoriser 500 homologues Secure Client (services client sécurisés) et 500 autres homologues VPN simultanément; ou 700 homologues Secure Client (services client sécurisés) et 300 autres VPN; ou utiliser les 1 000 pour Secure Client (services client sécurisés). Si vous dépassez le nombre total d'homologues VPN, vous pouvez surcharger l'ASA. Assurez-vous donc de dimensionner votre réseau de manière appropriée.

Équilibrage de la charge VPN

L'équilibrage de charges VPN nécessite une licence de cryptage renforcé (3DES/AES).

Licences VPN existantes

Reportez-vous au contrat de licence de l'utilisateur final supplémentaire pour Secure Client (services client sécurisés) pour obtenir tous les renseignements pertinents sur les licences.

Remarque La licence Secure Client Premier est la seule licence Secure Client (services client sécurisés) prise en charge pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante.

Licence de chiffrement

Si le cryptage renforcé est activé, vous ne pouvez pas utiliser DES.

Nombre total de sessions de mandataire TLS

Chaque session de mandataire TLS pour l'inspection vocale chiffrée est prise en compte dans la limite de licences TLS.

D'autres applications qui utilisent des sessions de mandataire TLS ne sont pas prises en compte dans la limite du TLS, par exemple, le mandataire Mobility Advantage (qui ne nécessite pas de licence).

Certaines applications peuvent utiliser plusieurs sessions pour une connexion. Par exemple, si vous configurez un téléphone avec un Cisco Unified Communications Manager principal et de secours, il y a 2 connexions de mandataire TLS.

Vous définissez indépendamment la limite de mandataire TLS à l'aide de la commande **tls-proxy maximum-sessions** ou dans ASDM, en utilisant le volet **Configuration > Firewall (Pare-feu) > Unified Communications (Communications unifiées) > TLS Proxy (Mandataire TLS)**. Pour afficher les limites de votre modèle, saisissez la commande **tls-proxy maximum-sessions ?**. Lorsque vous appliquez une licence de mandataire TLS supérieure à la limite de mandataire TLS par défaut, l'ASA définit automatiquement la

limite de mandataire TLS pour correspondre à la licence. La limite de mandataire TLS a priorité sur la limite de la licence; si vous définissez la limite de mandataire TLS pour qu'elle soit inférieure à la licence, vous ne pouvez pas utiliser toutes les sessions de votre licence.



Remarque Pour les licences dont la référence se termine par « K8 » (par exemple, les licences de moins de 250 utilisateurs), les sessions de mandataire TLS sont limitées à 1 000. Pour les licences dont la référence se termine par « K9 » (par exemple, les licences de 250 utilisateurs ou plus), la limite de mandataire TLS dépend de la configuration, jusqu'à la limite du modèle. K8 et K9 indiquent si la licence est restreinte pour l'exportation : la licence K8 n'est pas limitée tandis que la licence K9 est restreinte.

Si vous effacez la configuration (à l'aide de la commande **clear configure all**, par exemple), la limite de mandataire TLS est définie par défaut pour votre modèle; si cette valeur par défaut est inférieure à la limite de licence, vous verrez un message d'erreur pour utiliser la commande **tls-proxy maximum-sessions** afin d'augmenter à nouveau la limite (dans ASDM, utilisez le volet **TLS Proxy** (Mandataire TLS)). Si vous utilisez le basculement et saisissez la commande **write standby** ou dans ASDM, utilisez **File (Fichier) > Save Running Configuration to Standby Unit (Enregistrer la configuration d'exécution sur l'unité en veille)** sur l'unité principale pour forcer une synchronisation de la configuration; la commande **clear configure all** est générée automatiquement sur l'unité secondaire, vous pouvez donc voir le message d'avertissement sur l'unité secondaire. Étant donné que la synchronisation de la configuration restaure la limite de mandataire TLS définie sur l'unité principale, vous pouvez ignorer l'avertissement.

Vous pouvez également utiliser des sessions de chiffrement SRTP pour vos connexions :

- Pour les licences K8, les sessions SRTP sont limitées à 250.
- Pour les licences K9, il n'y a pas de limite.



Remarque Seuls les appels qui nécessitent un chiffrement ou un déchiffrement pour un support sont pris en compte dans la limite du SRTP; si la transmission est définie pour l'appel, même si les deux segments sont des SRTP, ils ne sont pas pris en compte dans la limite.

Nombre maximum de VLAN

Pour qu'une interface soit prise en compte dans la limite de VLAN, vous devez lui attribuer un VLAN.

Licences partagées Secure Client (services client sécurisés) Premium (AnyConnect 3 et versions antérieures)



Remarque La fonctionnalité de licence partagée sur l'ASA n'est pas prise en charge avec les licences AnyConnect 4 et ultérieures. Les licences Secure Client (services client sécurisés) sont partagées et ne nécessitent plus de serveur partagé ni de licence de participant.

Une licence partagée vous permet d'acheter un grand nombre de sessions Secure Client (services client sécurisés) Premium et de partager les sessions, selon les besoins, entre un groupe d'ASA en configurant l'un des ASA en tant que serveur de licences partagées et les autres en tant que participants aux licences partagées.

Licences de basculement

À quelques exceptions près, les unités de basculement ne nécessitent pas la même licence sur chaque unité. Pour les versions antérieures, consultez le document de licence de votre version.

Exigences et exceptions en matière de licence de basculement

Modèle	Exigence de licence
ISA 3000	Licence Security Plus sur les deux unités. **Remarque** Chaque unité doit avoir la même licence de chiffrement.

Remarque Une clé permanente valide est requise; dans de rares cas sur l'ISA 3000, votre clé d'authentification PAK peut être supprimée. Si votre clé est constituée uniquement de 0, vous devez réinstaller une clé d'authentification valide avant que le basculement puisse être activé.

Association des licences de basculement

Pour les paires de basculement, les licences de chaque unité sont combinées en une seule licence de grappe en cours d'exécution. Si vous achetez des licences distinctes pour chaque unité, la licence combinée utilise les règles suivantes :

- Pour les licences qui ont des niveaux numériques, comme le nombre de sessions, les valeurs des licences de chaque unité sont combinées jusqu'à la limite de la plateforme. Si toutes les licences utilisées sont à durée limitée, les licences sont décomptées simultanément.

  Par exemple, pour le basculement :

  - Vous avez deux ASA avec 10 sessions de mandataire TLS installées sur chacun; les licences seront combinées pour un total de 20 sessions de mandataire TLS.
  - Vous avez un ASA avec 1 000 sessions de mandataire TLS et un autre avec 2 000 sessions; comme la limite de plateformes est de 2 000, la licence combinée autorise 2 000 sessions de mandataire TLS.

- Pour les licences dont l'état est activé ou désactivé, la licence ayant l'état activé est utilisée.
- Pour les licences à durée limitée qui sont activées ou désactivées (et qui n'ont pas de niveaux numériques), la durée est la durée combinée de toutes les licences. L'unité principale/de contrôle compte d'abord sa licence, et à son expiration, l'unité secondaire/de données commence à décompter sa licence, et ainsi de suite.

Sujets connexes

Supervision des licences PAK, à la page 115

Perte de communication entre les unités de basculement

Si les unités perdent la communication pendant plus de 30 jours, chaque unité revient à la licence installée localement. Pendant le délai de grâce de 30 jours, la licence en cours d'exécution combinée continue d'être utilisée par toutes les unités.

Si vous rétablissez la communication pendant le délai de grâce de 30 jours, pour les licences à durée limitée, le temps écoulé est soustrait de la licence principale/de contrôle; si la licence principale/de contrôle expire, la licence secondaire/de données commence seulement à être décomptée.

Si vous ne rétablissez pas la communication pendant la période de 30 jours, pour les licences à durée limitée, le temps est soustrait de toutes les licences des unités, si elles sont installées. Elles sont traitées comme des licences distinctes et ne bénéficient pas de la licence combinée. Le délai écoulé comprend le délai de grâce de 30 jours.

Mise à niveau des paires de basculement

Étant donné que les paires de basculement ne nécessitent pas la même licence sur les deux unités, vous pouvez appliquer de nouvelles licences à chaque unité sans temps d'arrêt. Si vous appliquez une licence permanente qui nécessite un rechargement, vous pouvez basculer vers l'autre unité pendant le rechargement. Si les deux unités nécessitent un rechargement, vous pouvez les recharger séparément pour éviter les temps d'arrêt.

Sujets connexes

Activer ou désactiver les clés, à la page 107

Aucun modèle de chiffrement des données utiles

Vous pouvez acheter certains modèles sans chiffrement des données utiles. Pour l'exportation vers certains pays, le chiffrement des données utiles ne peut pas être activé sur la série ASA. Le logiciel ASA détecte un modèle sans chiffrement des données utiles et désactive les fonctionnalités suivantes :

- Communications unifiées
- VPN

Vous pouvez toujours installer la licence de cryptage renforcé (3DES/AES) pour l'utiliser avec les connexions de gestion. Par exemple, vous pouvez utiliser ASDM HTTPS/SSL, SSHv2, Telnet et SNMPv3.

Lorsque vous affichez la licence, les licences VPN et de communications unifiées ne seront pas répertoriées.

Sujets connexes

Supervision des licences PAK, à la page 115

FAQ sur les licences

Puis-je activer plusieurs licences à durée limitée?

Oui. Vous pouvez utiliser une seule licence à durée limitée par fonctionnalité à la fois.

Puis-je « cumuler » des licences à durée limitée afin que, lorsque la durée expire, la licence suivante soit automatiquement utilisée?

Oui. Pour les licences identiques, la durée est cumulée lorsque vous installez plusieurs licences à durée limitée. Pour les licences non identiques (par exemple, une licence Secure Client (services client sécurisés) Premium de 1 000 sessions et une licence de 2 500 sessions), l'ASA active automatiquement la licence à durée limitée suivante qu'il trouve pour la fonctionnalité.

Puis-je installer une nouvelle licence permanente tout en conservant une licence à durée limitée active?

Oui. L'activation d'une licence permanente n'affecte pas les licences à durée limitée.

Pour le basculement, puis-je utiliser un serveur de licences partagées comme unité principale et le serveur de sauvegarde de licences partagées comme unité secondaire?

Non. L'unité secondaire dispose de la même licence d'exécution que l'unité principale; dans le cas du serveur de licences partagées, une licence serveur est requise. Le serveur de sauvegarde nécessite une licence de participant. Le serveur de sauvegarde peut se trouver dans une paire de basculement distincte composée de deux serveurs de sauvegarde.

Dois-je acheter les mêmes licences pour l'unité secondaire d'une paire de basculement?

Non. À partir de la version 8.3(1), vous n'avez pas besoin d'avoir des licences correspondantes sur les deux unités. En règle générale, vous achetez une licence uniquement pour l'unité principale; l'unité secondaire hérite de la licence principale lorsqu'elle devient active. Dans le cas où vous avez également une licence distincte sur l'unité secondaire (par exemple, si vous avez acheté des licences correspondantes pour des logiciels antérieurs à la version 8.3), les licences sont combinées en une licence de grappe de basculement en cours d'exécution, jusqu'aux limites du modèle.

Puis-je utiliser une licence Secure Client (services client sécurisés) Premium à durée limitée ou permanente en plus d'une licence AnyConnect Premium partagée?

Oui. La licence partagée est utilisée uniquement après l'épuisement des sessions de la licence installée localement (à durée limitée ou permanente).

Remarque Sur le serveur de licences partagées, la licence Secure Client (services client sécurisés) Premium permanente n'est pas utilisée; vous pouvez toutefois utiliser une licence à durée limitée en même temps que la licence du serveur de licences partagées. Dans ce cas, les sessions de licence à durée limitée ne sont disponibles que pour les sessions Secure Client (services client sécurisés) Premium locales; elles ne peuvent pas être ajoutées au groupe de licences partagées pour être utilisées par les participants.

Lignes directrices relatives aux licences PAK

Directives relatives au mode contextuel

En mode de contexte multiple, appliquez la clé d'activation dans l'espace d'exécution du système.

Directives en matière de basculement

Consultez Licences de basculement, à la page 99.

Directives sur les modèles

- Les licences Smart sont prises en charge sur l'ASA virtuel uniquement.
- Les licences partagées ne sont pas prises en charge sur l'ASA virtuel, l'ASA 5506-X, l'ASA 5508-X et l'ASA 5516-X.
- Les ASA 5506-X et ASA 5506W-X ne prennent pas en charge les licences à durée limitée.

Lignes directrices relatives à la mise à niveau et à la rétrogradation

Votre clé d'activation reste compatible si vous effectuez une mise à niveau vers la dernière version à partir de n'importe quelle version précédente. Cependant, vous pourriez avoir des problèmes si vous souhaitez conserver la capacité de rétrogradation :

- Rétrogradation à la version 8.1 ou antérieure : après la mise à niveau, si vous activez des licences de fonctionnalités supplémentaires qui ont été introduites *avant la version 8.2*, la clé d'activation continue d'être compatible avec les versions antérieures si vous effectuez une rétrogradation. Cependant, si vous activez des licences de fonctionnalités qui ont été introduites dans la version *8.2 ou ultérieure*, la clé d'activation n'est pas rétrocompatible. Si vous avez une clé de licence incompatible, consultez les lignes directrices suivantes :
  - Si vous avez déjà saisi une clé d'activation dans une version antérieure, l'ASA utilise cette clé (sans aucune des nouvelles licences que vous avez activées dans la version 8.2 ou ultérieure).
  - Si vous avez un nouveau système et que vous n'avez pas de clé d'activation antérieure, vous devez demander une nouvelle clé d'activation compatible avec la version antérieure.
- Rétrogradation à la version 8.2 ou antérieure : la version 8.3 a introduit une utilisation plus robuste des clés temporelles ainsi que des modifications des licences de basculement :
  - Si vous avez plusieurs clés d'activation temporelles actives, lorsque vous effectuez une rétrogradation, seule la dernière clé temporelle activée peut être active. Toutes les autres clés sont désactivées. Si la dernière licence à durée limitée concerne une fonctionnalité introduite dans la version 8.3, cette licence reste toujours la licence active même si elle ne peut pas être utilisée dans les versions antérieures. Saisissez la clé permanente ou une clé temporelle valide.
  - Si vous avez des licences incompatibles avec une paire de basculement, la rétrogradation désactivera le basculement. Même si les clés correspondent, la licence utilisée ne sera plus une licence combinée.
  - Si vous avez installé une licence à durée limitée, mais qu'elle concerne une fonctionnalité introduite dans la version 8.3, cette licence à durée limitée restera active après la rétrogradation. Vous devez saisir à nouveau la clé permanente pour désactiver la licence à durée limitée.

Directives supplémentaires

- La clé d'activation n'est pas stockée dans votre fichier de configuration; elle est stockée sous forme de fichier caché dans la mémoire flash.
- La clé d'activation est liée au numéro de série de l'appareil. Les licences de fonctionnalités ne peuvent pas être transférées entre les périphériques (sauf en cas de défaillance matérielle). Si vous devez remplacer votre périphérique en raison d'une défaillance matérielle et qu'il est couvert par le TAC de Cisco, communiquez avec l'équipe chargée des licences de Cisco afin de transférer votre licence existante vers

le nouveau numéro de série. L'équipe chargée des licences de Cisco vous demandera le numéro de référence de la clé d'autorisation du produit et le numéro de série existant.

- Le numéro de série utilisé pour la licence est celui indiqué sur la page de la clé d'activation. Ce numéro de série est différent de celui du châssis indiqué à l'extérieur du matériel. Le numéro de série du châssis est utilisé pour l'assistance technique, mais pas pour les licences.
- Une fois achetée, vous ne pouvez pas retourner une licence pour obtenir un remboursement ou une licence mise à niveau.
- Sur une seule unité, vous ne pouvez pas ajouter deux licences distinctes pour la même fonctionnalité; par exemple, si vous achetez une licence SSL VPN de 25 sessions, puis achetez ultérieurement une licence de 50 sessions, vous ne pouvez pas utiliser 75 sessions; vous pouvez utiliser un maximum de 50 sessions. (Vous pourriez acheter une licence plus importante à un prix de mise à niveau, par exemple de 25 à 75 sessions; ce type de mise à niveau doit se différencier de l'ajout de deux licences distinctes).
- Bien que vous puissiez activer tous les types de licence, certaines fonctionnalités sont incompatibles entre elles. Dans le cas de la licence AnyConnect Essentials, la licence est incompatible avec les licences suivantes : licence AnyConnect Premium, licence AnyConnect Premium partagée et licence d'évaluation de point d'accès avancée. Par défaut, si vous installez la licence AnyConnect Essentials (si elle est disponible pour votre modèle), elle est utilisée à la place des licences ci-dessus. Vous pouvez désactiver la licence AnyConnect Essentials dans la configuration pour restaurer l'utilisation des autres licences à l'aide du volet **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau (client)) > Advanced (Avancé) > AnyConnect Essentials**.

Configurer les licences PAK

Cette section décrit comment obtenir une clé d'activation et comment l'activer. Vous pouvez également désactiver une clé.

Commander des licences PAK et obtenir une clé d'activation

Pour installer une licence sur l'ASA, vous avez besoin de clés d'autorisation de produit, que vous pouvez ensuite enregistrer auprès de Cisco.com pour obtenir une clé d'activation. Vous pouvez ensuite saisir la clé d'activation sur l'ASA. Vous avez besoin d'une clé d'autorisation de produit distincte pour chaque licence de fonctionnalité. Les clés PAK sont combinées pour vous donner une clé d'activation unique. Vous avez peut-être reçu toutes vos clés de licence PAK dans la boîte de votre appareil. L'ASA dispose de la licence de base ou Security Plus, ainsi que de la licence de cryptage renforcé (3DES/AES), si vous remplissez les conditions requises pour son utilisation. Si vous devez demander manuellement la licence de cryptage renforcé (qui est gratuite), consultez la page http://www.cisco.com/go/license.

Avant de commencer

Lorsque vous achetez une ou plusieurs licences pour l'appareil, vous les gérez dans le Cisco Smart Software Manager :

https://software.cisco.com/#module/SmartLicensing

Si vous n'avez pas encore de compte, configurez un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.

Procédure

Étape 1 Pour acheter des licences supplémentaires, rendez-vous sur http://www.cisco.com/go/ccw. Consultez le guide de commande et la FAQ Secure Client (services client sécurisés) suivants :

- Guide de commande Cisco Secure Client (services client sécurisés)
- Foire aux questions (FAQ) Secure Client (services client sécurisés) Licensing

Après avoir commandé une licence, vous recevrez un courriel avec une clé d'autorisation de produit (PAK). Pour les licences Secure Client (services client sécurisés), vous recevez une clé PAK multiutilisation que vous pourrez appliquer à plusieurs ASA partageant le même ensemble de séances de l'utilisateur. Le courriel de la PAK peut prendre plusieurs jours dans certains cas.

Étape 2 Obtenez le numéro de série de votre ASA en sélectionnant **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Activation Key (Clé d'activation)** (en mode de contexte multiple, affichez le numéro de série dans l'espace d'exécution du système).

Le numéro de série utilisé pour la licence est différent de celui du châssis indiqué à l'extérieur du matériel. Le numéro de série du châssis est utilisé pour l'assistance technique, mais pas pour les licences.

Étape 3 Pour obtenir la clé d'activation, accédez au site Web de la licence suivant :

http://www.cisco.com/go/license

Étape 4 Saisissez les renseignements suivants lorsque vous y êtes invité :

- Clé d'autorisation de produit (si vous avez plusieurs clés, saisissez d'abord l'une des clés. Vous devez saisir chaque clé en tant que processus distinct.)
- Le numéro de série de votre ASA
- Votre adresse courriel

Une clé d'activation est automatiquement générée et envoyée à l'adresse courriel que vous fournissez. Cette clé comprend toutes les fonctionnalités que vous avez enregistrées jusqu'à présent pour les licences permanentes. En ce qui concerne les licences à durée déterminée, chacune possède une clé d'activation distincte.

Étape 5 Si vous disposez de clés d'autorisation de produit supplémentaires, répétez le processus pour chaque clé d'autorisation de produit. Après avoir saisi toutes les clés d'autorisation de produit, la clé d'activation finale fournie comprend toutes les fonctionnalités permanentes que vous avez enregistrées.

Étape 6 Installez la clé d'activation conformément à Activer ou désactiver les clés, à la page 107.

Obtenir une licence de cryptage renforcé

Pour utiliser ASDM (et de nombreuses autres fonctionnalités), vous devez installer la licence de cryptage renforcé (3DES/AES). Si votre ASA n'est pas livré avec la licence de cryptage renforcé préinstallée, vous pouvez en demander une gratuitement. Vous devez bénéficier d'une licence de cryptage renforcé en fonction de votre pays.

Procédure

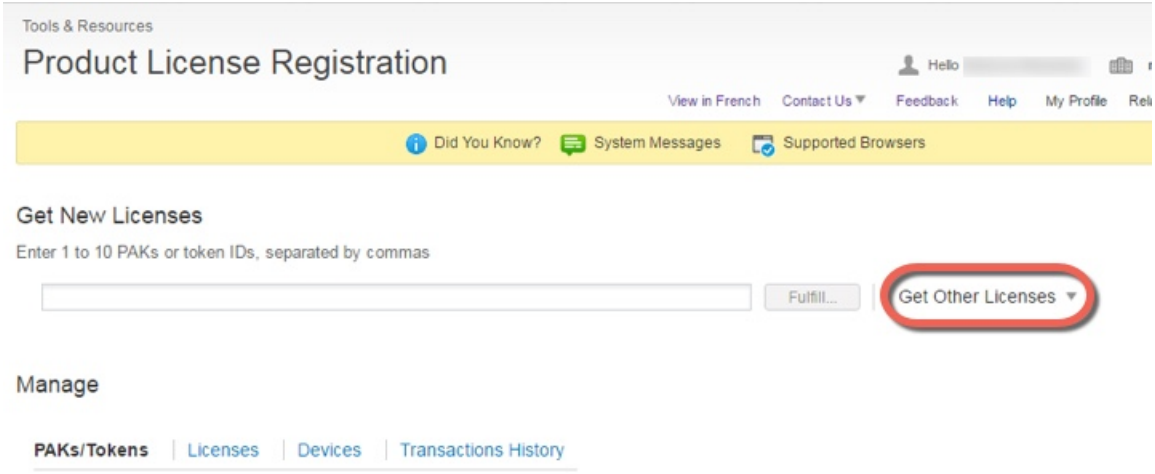
Étape 1 Utilisez la commande suivante pour obtenir le numéro de série de votre ASA :

show version | grep Serial

Ce numéro de série est différent de celui du châssis indiqué à l'extérieur du matériel. Le numéro de série du châssis est utilisé pour l'assistance technique, mais pas pour les licences.

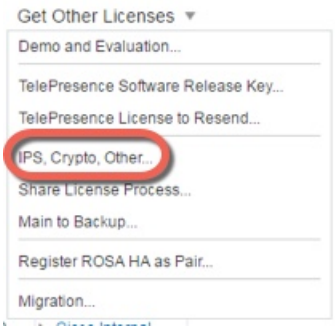
Étape 2 Consultez https://www.cisco.com/go/license, puis cliquez sur **Get Other Licenses** (Obtenir d'autres licences).

Illustration 10 : Get Other Licenses (obtenir d'autres licences)



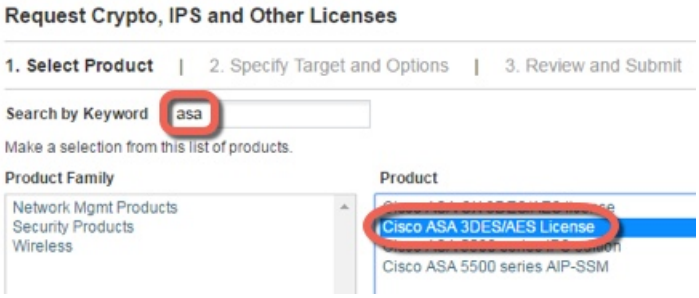
Étape 3 Choisissez **IPS, Crypto, Other**.

Illustration 11 : IPS, Crypto, Othe (IPS, cryptage, autre)



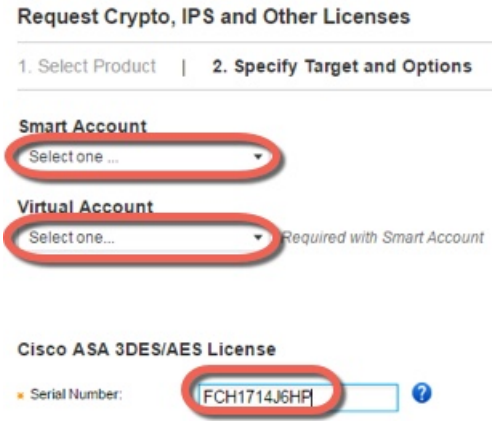
Étape 4 Dans le champ de recherche par mot clé **Search by Keyword** (Rechercher par mot clé), entrez **asa** et sélectionnez **Cisco ASA 3DES/AES License** (Licence Cisco ASA 3DES/AES).

Illustration 12 : Licence Cisco ASA 3DES/AES



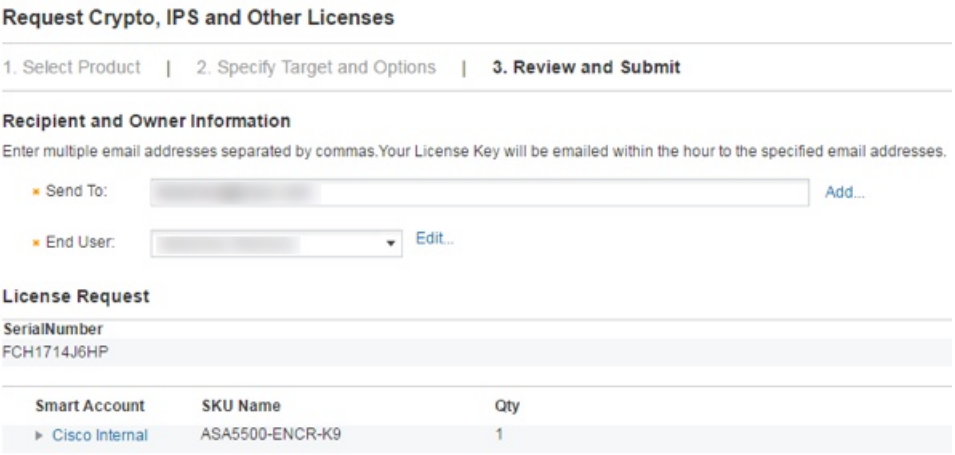
Étape 5 Sélectionnez votre **Smart Account** (Compte Smart) et votre **Virtual Account** (Compte virtuel), entrez le **Serial Number** (Numéro de série) de l'ASA, puis cliquez sur **Next** (Suivant) pour passer à l'étape suivante.

Illustration 13 : Smart Account (Compte Smart), Virtual Account (Compte virtuel) et Serial Number (Numéro de série)



Étape 6 L'adresse courriel du destinataire et le nom de l'utilisateur final sont automatiquement remplis. Si nécessaire, entrez les autres adresses courriel requises. Cochez la case **I Agree** (J'accepte) pour indiquer votre accord, puis cliquez sur **Submit** (Envoyer) pour envoyer le tout.

Illustration 14 : Submit (envoyer)



Étape 7 Vous recevrez alors un courriel contenant la clé d'activation, mais vous pouvez aussi la télécharger immédiatement depuis la zone de gestion des licences **Manage (Gérer)** > **Licenses (Licences)**.

Étape 8 Appliquez la clé d'activation conformément à Activer ou désactiver les clés, à la page 107.

Activer ou désactiver les clés

Cette section décrit comment saisir une nouvelle clé d'activation et comment activer et désactiver les clés à durée déterminée.

Avant de commencer

- Si vous êtes déjà en mode de contexte multiple, entrez la clé d'activation dans l'espace d'exécution du système.
- Certaines licences permanentes nécessitent que vous rechargiez l'ASA après les avoir activées. Le tableau suivant répertorie les licences qui nécessitent un rechargement.

Tableau 8 : Exigences en matière de rechargement de la licence permanente

Modèle	Action de licence nécessitant un rechargement
Tous les modèles	Rétrogradation de la licence de chiffrement.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)**, puis dans le volet **Licensing (Licences)** > **Activation Key (Clé d'activation)** ou **Licensing Activation Key (Clé d'activation de licence)**, selon votre modèle.

Étape 2 Pour saisir une nouvelle clé d'activation, permanente ou à durée déterminée, saisissez la nouvelle clé d'activation dans le champ **New Activation Key** (Nouvelle clé d'activation).

La clé est une chaîne hexadécimale de cinq éléments avec un espace entre chaque élément. Le spécificateur 0x de début est facultatif; toutes les valeurs sont censées être hexadécimales. Par exemple :

```
ASA0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

Vous pouvez installer une clé permanente et plusieurs clés à durée déterminée. Si vous entrez une nouvelle clé permanente, celle-ci remplacera la clé déjà installée. Si vous saisissez une nouvelle clé à durée déterminée, elle est active par défaut et s'affiche dans le tableau des clés de licence à durée limitée installées. La dernière clé à durée déterminée que vous activez pour une fonctionnalité donnée est la clé active.

Étape 3 Pour activer ou désactiver une clé à durée déterminée, choisissez la clé dans le tableau des **clés de licence à durée limitée installées**, puis cliquez sur **Activate** (Activer) ou **Deactivate** (Désactiver).

Vous ne pouvez avoir qu'une seule clé à durée déterminée active pour chaque fonctionnalité.

Étape 4 Cliquez sur **Update Activation Key** (Mettre à jour la clé d'activation).

Certaines licences permanentes nécessitent que vous rechargiez l'ASA après avoir saisi la nouvelle clé d'activation. Vous serez invité à le recharger, le cas échéant.

Sujets connexes

Licences à durée limitée, à la page 94

Configurer une licence partagée (Secure Client (services client sécurisés) 3 et versions antérieures)

Remarque La fonctionnalité de licence partagée sur l'ASA n'est pas prise en charge avec les licences Secure Client (services client sécurisés) 4 et ultérieures. Les licences Secure Client (services client sécurisés) sont partagées et ne nécessitent plus de serveur partagé ni de licence de participant.

Cette section décrit comment configurer le serveur de licences partagées et les participants.

À propos des licences partagées

Une licence partagée vous permet d'acheter un grand nombre de sessions Secure Client (services client sécurisés) Premium et de partager les sessions, selon les besoins, entre un groupe d'ASA en configurant l'un des ASA en tant que serveur de licences partagées et les autres en tant que participants aux licences partagées.

À propos du serveur de licences partagées et des participants

Les étapes suivantes décrivent le fonctionnement des licences partagées :

1. Décidez quel ASA doit être le serveur de licences partagées et achetez la licence de serveur de licences partagées en utilisant ce numéro de série de périphérique.
2. Décidez quels ASA doivent être des participants à une licence partagée, y compris le serveur de sauvegarde à licence partagée, et obtenez une licence de participant à une licence partagée pour chaque périphérique, en utilisant le numéro de série de chaque périphérique.
3. (Facultatif) Désignez un deuxième ASA comme serveur de sauvegarde de licences partagées. Vous ne pouvez définir qu'un seul serveur de sauvegarde.

Remarque Le serveur de sauvegarde de licences partagées n'a besoin que d'une licence de participant.

4. Configurez un secret partagé sur le serveur de licences partagées; tous les participants ayant le secret partagé peuvent utiliser la licence partagée.
5. Lorsque vous configurez l'ASA en tant que participant, il s'enregistre auprès du serveur de licences partagées en envoyant des renseignements sur lui-même, y compris la licence locale et les renseignements sur le modèle.

Remarque Le participant doit pouvoir communiquer avec le serveur sur le réseau IP; il ne doit pas être sur le même sous-réseau.

6. Le serveur de licences partagées répond par des renseignements sur la fréquence à laquelle le participant doit interroger le serveur.
7. Lorsqu'un participant utilise les sessions de la licence locale, il envoie une demande au serveur de licences partagées pour des sessions supplémentaires par incréments de 50 sessions.
8. Le serveur de licences partagées répond par une licence partagée. Le nombre total de sessions utilisées par un participant ne peut pas dépasser le nombre maximal de sessions pour le modèle de plateforme.

Remarque Le serveur de licences partagées peut également participer au regroupement de licences partagées. Il n'a pas besoin de licence de participant et de licence de serveur pour y participer.

1. S'il ne reste pas assez de sessions dans le groupe de licences partagées pour le participant, le serveur répond par autant de sessions que disponible.
2. Le participant continue d'envoyer des messages d'actualisation pour demander plus de sessions jusqu'à ce que le serveur puisse répondre de manière adéquate à la demande.

9. Lorsque la charge est réduite sur un participant, il envoie un message au serveur pour libérer les sessions partagées.

Remarque L'ASA utilise le protocole SSL entre le serveur et le participant pour chiffrer toutes les communications.

Problèmes de communication entre le participant et le serveur

Consultez les lignes directrices suivantes pour résoudre les problèmes de communication entre le participant et le serveur :

- Si un participant ne parvient pas à envoyer une actualisation après trois fois l'intervalle d'actualisation, le serveur libère les sessions dans le groupe de licences partagées.
- Si le participant ne parvient pas à atteindre le serveur de licences pour envoyer l'actualisation, il peut continuer à utiliser la licence partagée qu'il a reçue du serveur pendant un délai de 24 heures.
- Si le participant n'est toujours pas en mesure de communiquer avec un serveur de licences après 24 heures, le participant libère la licence partagée, même s'il a toujours besoin des sessions. Le participant laisse les connexions existantes établies, mais ne peut pas accepter de nouvelles connexions au-delà de la limite de licence.
- Si un participant se reconnecte au serveur avant l'expiration du délai de 24 heures, mais après l'expiration des sessions du participant par le serveur, le participant doit envoyer une nouvelle demande pour les sessions; le serveur répond avec autant de sessions que possible pouvant être réattribuées à ce participant.

À propos du serveur de sauvegarde de licences partagées

Le serveur de sauvegarde de licences partagées doit s'enregistrer auprès du serveur de licences partagées principal avant de pouvoir assumer son rôle de sauvegarde. Lors de l'enregistrement, le serveur de licences partagées principal synchronise les paramètres de serveur ainsi que les renseignements de licence partagée avec la sauvegarde, y compris une liste des participants inscrits et l'utilisation actuelle des licences. Le serveur principal et le serveur de sauvegarde synchronisent les données à des intervalles de 10 secondes. Après la synchronisation initiale, le serveur de sauvegarde peut effectuer des tâches de sauvegarde avec succès, même après un rechargement.

Lorsque le serveur principal tombe en panne, le serveur de sauvegarde prend le relais du fonctionnement du serveur. Le serveur de sauvegarde peut fonctionner jusqu'à 30 jours consécutifs, après quoi serveur de sauvegarde arrête d'émettre des sessions aux participants et les sessions existantes expirent. Assurez-vous de réinitialiser le serveur principal dans ce délai de 30 jours. Les messages de journal système de niveau critique sont envoyés à 15 jours et à nouveau à 30 jours.

Lorsque le serveur principal est remis en service, il se synchronise avec le serveur de sauvegarde, puis prend le relais du fonctionnement du serveur.

Lorsque le serveur de sauvegarde n'est pas actif, il agit comme un participant régulier du serveur de licences partagées principal.

Remarque Lorsque vous lancez le serveur de licences partagées principal pour la première fois, le serveur de sauvegarde ne peut fonctionner indépendamment que pendant 5 jours. La limite opérationnelle augmente de jour en jour jusqu'à 30 jours. De plus, si le serveur principal tombe en panne ultérieurement, la limite opérationnelle du serveur de sauvegarde diminuera de jour en jour. Lorsque le serveur principal est remis en service, le serveur de sauvegarde recommence à augmenter de jour en jour. Par exemple, si le serveur principal est en panne pendant 20 jours et que le serveur de sauvegarde est actif pendant ce temps, le serveur de sauvegarde n'aura plus qu'une limite de 10 jours. Le serveur de sauvegarde se « recharge » jusqu'à 30 jours après 20 jours supplémentaires en tant que sauvegarde inactive. Cette fonction de rechargement est mise en œuvre pour décourager toute utilisation abusive de la licence partagée.

Licences de basculement et partagées

Cette section décrit comment les licences partagées interagissent avec le basculement.

Serveurs de licences de basculement et partagées

Cette section décrit comment le serveur principal et le serveur de sauvegarde interagissent avec le basculement. Étant donné que le serveur de licences partagées remplit également les fonctions normales de l'ASA, notamment celles de passerelle VPN et de pare-feu, il peut être nécessaire de configurer le basculement pour les serveurs de licences partagés principal et de secours afin d'améliorer la fiabilité.

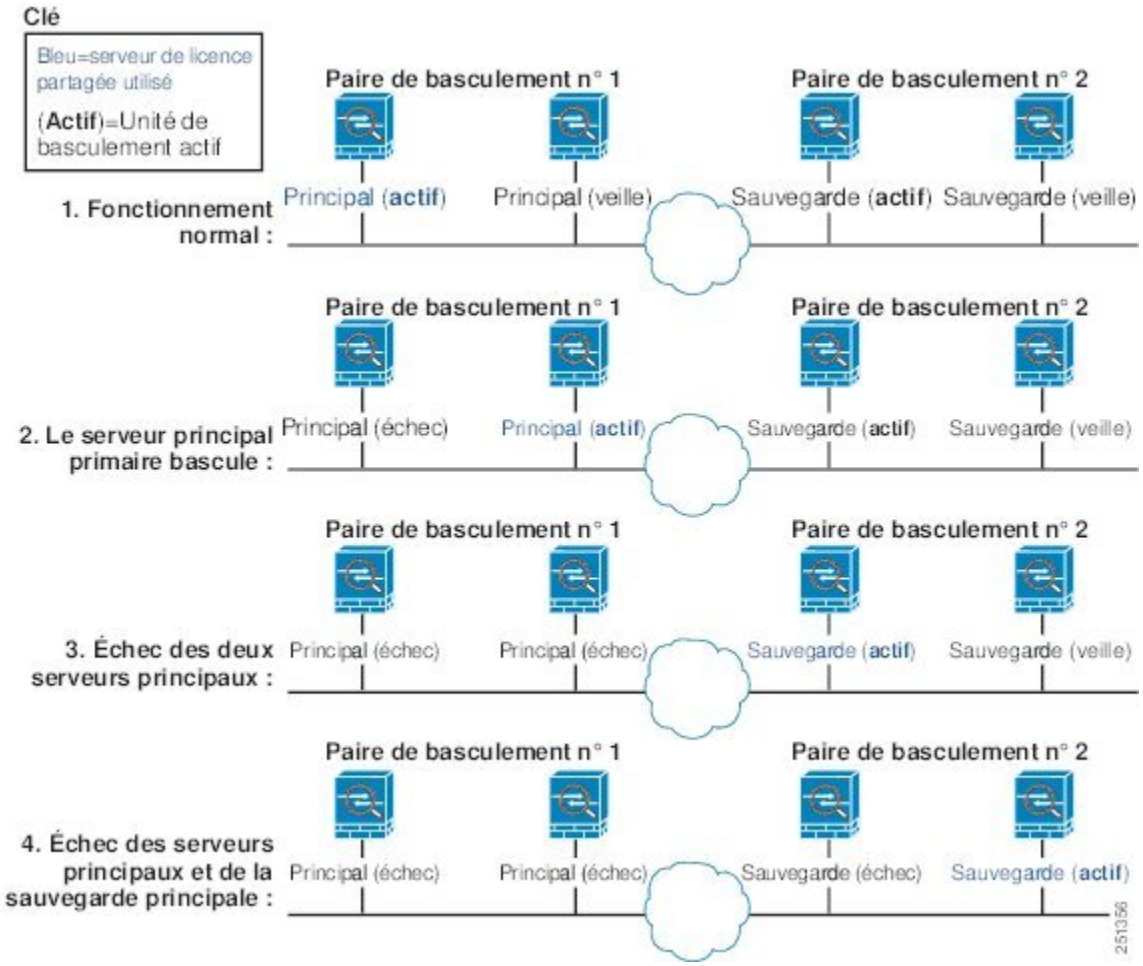
Remarque Le mécanisme du serveur de sauvegarde est distinct du basculement, mais compatible avec celui-ci.

Les licences partagées ne sont prises en charge qu'en mode de contexte unique, de sorte que le basculement actif/actif n'est pas pris en charge.

Pour le basculement actif/veille, l'unité principale agit en tant que serveur de licences partagées principal et l'unité de secours agit en tant que serveur de licences partagées principal après le basculement. L'unité de secours ne sert *pas* de serveur de licences partagées de secours. Au lieu de cela, vous pouvez avoir une deuxième paire d'unités agissant en tant que serveur de sauvegarde, si vous le souhaitez.

Par exemple, vous avez un réseau avec 2 paires de basculement. La paire n° 1 comprend le serveur de licences principal. La paire n° 2 comprend le serveur de sauvegarde. Lorsque l'unité principale de la paire n° 1 tombe en panne, l'unité en veille devient immédiatement le nouveau serveur de licences principal. Le serveur de sauvegarde de la paire n° 2 n'est jamais utilisé. Ce n'est que si les deux unités de la paire n° 1 tombent en panne que le serveur de sauvegarde de la paire n° 2 est utilisé comme serveur de licences partagées. Si la paire n° 1 reste en panne et que l'unité principale de la paire n° 2 tombe en panne, l'unité en veille de la paire n° 2 sert de serveur de licences partagées (voir la figure suivante).

Illustration 15 : Serveurs de licences de basculement et partagées



Le serveur de sauvegarde de secours partage les mêmes limites opérationnelles que le serveur de sauvegarde principal; si l'unité en veille devient active, elle continue le compte à rebours là où l'unité principale s'est arrêtée.

Sujets connexes

À propos du serveur de sauvegarde de licences partagées, à la page 110

Participants aux licences de basculement et partagées

Pour les paires de participants, les deux unités s'enregistrent auprès du serveur de licences partagées en utilisant des ID de participant distincts. L'unité active synchronise son ID de participant avec l'unité de sauvegarde. L'unité de sauvegarde utilise cet ID pour générer une demande de transfert lorsqu'elle passe au rôle actif. Cette demande de transfert est utilisée pour déplacer les sessions partagées de l'unité précédemment active vers la nouvelle unité active.

Nombre maximum de participants

L'ASA ne limite pas le nombre de participants pour la licence partagée; cependant, un très grand réseau partagé peut potentiellement affecter les performances du serveur de licences. Dans ce cas, vous pouvez augmenter le délai entre les actualisations des participants ou créer deux réseaux partagés.

Configurer le serveur de licences partagées

Cette section décrit comment configurer l'ASA pour qu'il soit un serveur de licences partagées.

Avant de commencer

Le serveur doit avoir une clé de serveur de licences partagées.

Procédure

Étape 1 Choisissez le volet **Configuration** > **Device Management (Gestion des périphériques)** > **Licenses (Licences)** > **Shared SSL VPN Licenses (Licences SSL VPN partagées)**.

Étape 2 Dans le champ **Shared Secret** (Secret partagé), saisissez le secret partagé sous la forme d'une chaîne composée de 4 à 128 caractères ASCII.

Tous les participants disposant de ce secret peuvent utiliser le serveur de licence.

Étape 3 (Facultatif) Dans le champ **TCP IP Port** (Port IP TCP), saisissez le port sur lequel le serveur écoute les connexions SSL des participants, entre 1 et 65 535.

La valeur par défaut est le port TCP 50554.

Étape 4 (Facultatif) Dans le champ **Refresh interval** (Intervalle d'actualisation), saisissez l'intervalle d'actualisation entre 10 et 300 secondes.

Cette valeur est fournie aux participants pour définir la fréquence à laquelle ils doivent communiquer avec le serveur. La valeur par défaut est de 30 secondes.

Étape 5 Dans la zone **Interfaces that serve shared licenses** (Interfaces qui servent des licences partagées), cochez la case **Shares Licenses** (Partage de licences) pour toutes les interfaces sur lesquelles les participants communiquent avec le serveur.

Étape 6 (Facultatif) Pour identifier un serveur de sauvegarde, dans la zone **Optional backup shared SSL VPN license server** (Serveur de sauvegarde de licences SSL VPN partagées facultatif) :

a) Dans le champ **Backup server IP address** (Adresse IP du serveur de sauvegarde), saisissez l'adresse IP du serveur de sauvegarde.

b) Dans le champ **Primary backup server serial number** (Numéro de série du serveur de sauvegarde principal), saisissez le numéro de série du serveur de sauvegarde.

c) Si le serveur de sauvegarde fait partie d'une paire de basculement, identifiez le numéro de série de l'unité de secours dans le champ **Secondary backup server serial number** (Numéro de série du serveur de sauvegarde secondaire).

Vous ne pouvez identifier qu'un seul serveur de sauvegarde et son unité de secours facultative.

Étape 7 Cliquez sur **Apply** (Appliquer).

Configurer le participant à la licence partagée et le serveur de sauvegarde facultatif

Cette section configure un participant de licence partagée pour communiquer avec le serveur de licences partagées. Elle décrit également comment configurer le participant en tant que serveur de sauvegarde, si nécessaire.

Avant de commencer

Le participant doit avoir une clé de participant à la licence partagée.

Procédure

Étape 1 Choisissez le volet **Configuration** > **Device Management (Gestion des périphériques)** > **Licenses (Licences)** > **Shared SSL VPN Licenses (Licences SSL VPN partagées)**.

Étape 2 Dans le champ Shared Secret (Secret partagé), saisissez le secret partagé sous la forme d'une chaîne composée de 4 à 128 caractères ASCII.

Étape 3 (Facultatif) Dans le champ TCP IP Port (Port IP TCP), saisissez le port sur lequel communiquer avec le serveur à l'aide de SSL, entre 1 et 65535.

La valeur par défaut est le port TCP 50554.

Étape 4 (Facultatif) Pour identifier le participant en tant que serveur de sauvegarde, dans la zone Select backup role of participant (Sélectionner le rôle de sauvegarde du participant) :

a) Cliquez sur le bouton radio **Backup Server** (Serveur de sauvegarde).
b) Cochez la case **Shares Licenses** (Licences partagées) pour toutes les interfaces sur lesquelles les participants communiquent avec le serveur de sauvegarde.

Étape 5 Cliquez sur **Apply** (Appliquer).

Licences de fonctionnalités prises en charge par modèle

Cette section décrit les licences disponibles pour chaque modèle et fournit des remarques importantes concernant les licences.

Licences par modèle

Cette section répertorie les licences de fonctionnalités disponibles pour chaque modèle :

Les éléments en *italique* sont des licences facultatives distinctes qui peuvent remplacer la version de licence de base (ou Security Plus, etc.). Vous pouvez combiner les licences facultatives.

Remarque Certaines fonctionnalités sont incompatibles entre elles. Consultez les chapitres consacrés aux différentes fonctionnalités pour obtenir des renseignements sur la compatibilité.

Si vous avez un modèle sans chiffrement des données utiles, certaines des fonctionnalités ci-dessous ne sont pas prises en charge. Consultez Aucun modèle de chiffrement des données utiles, à la page 100 pour obtenir la liste des fonctionnalités non prises en charge.

Pour de plus amples renseignements sur les licences, consultez Remarques relatives à la licence, à la page 96.

Fonctionnalités de la licence ISA 3000

Le tableau suivant présente les fonctionnalités sous licence pour l'ISA 3000.

Licences	Licence de base		Security Plus License	
Licences de pare-feu				
Filtre de trafic de réseau de zombies	Aucune assistance		Aucune assistance	
Connexions de pare-feu, simultanées	20 000		50 000	
Carrier (exploitant)	Aucune assistance		Aucune assistance	
Nombre total de sessions de mandataire TLS	160		160	
Licences VPN				
Homologues Secure Client (services client sécurisés)	Désactivé	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement : 25 maximum*	Désactivé	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement : 25 maximum*
Autres homologues VPN	10		50	
Total des homologues VPN, tous types combinés	25		50	
Équilibrage de la charge VPN	Aucune assistance		Aucune assistance	
Licences générales				
Chiffrement	Base (DES)	*Licence opt. : renforcé (3DES/AES)*	Base (DES)	*Licence opt. : renforcé (3DES/AES)*

Licences	Licence de base	Security Plus License
Basculement	Aucune assistance	Actif/Veille
Contextes de sécurité	Aucune assistance	Aucune assistance
Mise en grappe	Aucune assistance	Aucune assistance
Nombre maximum de VLAN	5	25

Supervision des licences PAK

Cette section décrit comment afficher les informations sur la licence.

Affichage de votre licence actuelle

Cette section décrit comment afficher votre licence actuelle et, pour les clés d'activation à durée limitée, le temps restant de la licence.

Avant de commencer

Si vous avez un modèle sans chiffrement des données utiles, vous affichez la licence, les licences VPN et de communications unifiées ne seront pas répertoriées. Consultez Aucun modèle de chiffrement des données utiles, à la page 100 pour de plus amples renseignements.

Procédure

Étape 1 Pour afficher la licence en cours d'exécution, qui est une combinaison de la licence permanente et de toutes les licences actives basées sur le temps, choisissez le volet **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Activation Key (Clé d'activation)** et affichez la zone Running Licenses (Licences en cours d'exécution).

En mode de contexte multiple, affichez la clé d'activation dans l'espace d'exécution du système en sélectionnant le volet **Configuration > Device Management (Gestion des périphériques) > Activation Key (Clé d'activation)**.

Pour une paire de basculement, la licence en cours d'exécution affichée est la licence combinée des unités principale et secondaire. Consultez Association des licences de basculement, à la page 99 pour de plus amples renseignements. Pour les licences à durée limitée avec des valeurs numériques (la durée n'est pas combinée), la colonne License Duration (Durée de la licence) affiche la licence à durée limitée la plus courte de l'unité principale ou secondaire; à l'expiration de cette licence, la durée de la licence de l'autre unité s'affiche.

Étape 2 (Facultatif) Pour afficher les détails de la licence à durée limitée, tels que les fonctionnalités incluses dans la licence et la durée, dans la zone Time-Based License Keys Installed (Clés de licence à durée limitée installées), choisissez une clé de licence, puis cliquez sur **Show License Details** (Afficher les détails de la licence).

Étape 3 (Facultatif) Pour une unité de basculement, afin d'afficher la licence installée sur cette unité (et non la licence combinée des unités principale et secondaire), dans la zone Running Licenses (Licences en cours d'exécution),

cliquez sur **Show information of license specifically purchased for this device alone** (Afficher les renseignements de licence spécifiquement achetée pour ce périphérique uniquement).

Supervision de la licence partagée

Pour superviser la licence partagée, choisissez **Monitoring (Supervision) > VPN > Clientless SSL VPN (SSL VPN sans client) > Shared Licenses (Licences partagées)**.

Historique des licences PAK

Nom de la caractéristique	Versions de plateforme	Description
Augmentation du nombre de connexions et de VLAN	7.0(5)	Augmentation des limites suivantes : • Connexions de licence de base ASA 5510 de 32 000 à 50 000; réseaux VLAN de 0 à 10. • Connexions de licence ASA 5510 Security Plus de 64 000 à 130 000; réseaux VLAN de 10 à 25. • Connexions ASA 5520 de 130 000 à 280 000; réseaux VLAN de 25 à 100. • Connexions ASA 5540 de 280 000 à 400 000; réseaux VLAN de 100 à 200.
Licences SSL VPN	7.1(1)	Des licences SSL VPN ont été introduites.
Augmentation du nombre de licences SSL VPN	7.2(1)	Une licence SSL VPN de 5 000 utilisateurs a été introduite pour les ASA 5550 et versions ultérieures.
Augmentation du nombre d'interfaces pour la licence de base sur l'ASA 5510	7.2(2)	Pour la licence de base sur l'ASA 5510, le nombre maximum d'interfaces est passé de 3 plus une interface de gestion à un nombre illimité d'interfaces.

Nom de la caractéristique	Versions de plateforme	Description
Augmentation du nombre de VLAN	7.2(2)	Le nombre maximum de VLAN pour la licence Security Plus sur l'ASA 5505 est passé de 5 (3 entièrement fonctionnels; 1 de basculement; un limité à une interface de secours) à 20 interfaces entièrement fonctionnelles. De plus, le nombre de ports de liaison est passé de 1 à 8. Il existe maintenant 20 interfaces entièrement fonctionnelles. Vous n'avez pas besoin d'utiliser la commande d'interface de sauvegarde pour chiffrer une interface ISP de secours; vous pouvez utiliser une interface entièrement fonctionnelle à cette fin. La commande d'interface de sauvegarde est toujours utile pour une configuration Easy VPN. Les limites de VLAN ont également été augmentées pour l'ASA 5510 (de 10 à 50 pour la licence de base et de 25 à 100 pour la licence Security Plus), l'ASA 5520 (de 100 à 150), l'ASA 5550 (de 200 à 250).
Prise en charge de Gigabit Ethernet pour la licence Security Plus sur l'ASA 5510	7.2(3)	L'ASA 5510 prend désormais en charge Gigabit Ethernet (1 000 Mbit/s) pour les ports Ethernet 0/0 et 0/1 avec la licence Security Plus. Dans la licence de base, ils continuent d'être utilisés comme ports Fast Ethernet (100 Mbit/s). Ethernet 0/2, 0/3 et 0/4 restent des ports Fast Ethernet pour les deux licences. **Remarque** Les noms d'interface restent Ethernet 0/0 et Ethernet 0/1.
Licence d'évaluation de point d'accès avancée	8.0(2)	Licence d'évaluation de point d'accès avancée a été introduite. Comme condition à l'achèvement d'une connexion Cisco AnyConnect ou d'une connexion SSL VPN sans client, l'ordinateur distant analyse une série considérablement élargie d'applications antivirus et anti-logiciel espion, de pare-feu, de systèmes d'exploitation et de mises à jour associées. Il analyse également les entrées de registre, les noms de fichiers et les noms de processus que vous spécifiez. Il envoie les résultats de l'analyse à l'ASA. L'ASA utilise les coordonnées de connexion de l'utilisateur et les résultats de l'analyse de l'ordinateur pour attribuer une politique d'accès dynamique (DAP). Avec une licence d'évaluation de point d'accès avancée, vous pouvez améliorer l'analyse de l'hôte en configurant une tentative de mise à jour des ordinateurs non conformes pour répondre aux exigences de la version. Cisco peut fournir des mises à jour en temps opportun de la liste des applications et des versions prises en charge par l'analyse de l'hôte dans un progiciel distinct de Cisco Secure Desktop.
Équilibrage de charges du VPN pour l'ASA 5510	8.0(2)	L'équilibrage de charges du VPN est désormais pris en charge sur la licence Security Plus de l'ASA 5510.

Nom de la caractéristique	Versions de plateforme	Description
Licence AnyConnect pour mobile	8.0(3)	La licence AnyConnect pour mobile a été introduite. Elle permet aux périphériques mobiles Windows de se connecter à l'ASA à l'aide du Secure Client (services client sécurisés).
Licences à durée limitée	8.0(4)/8.1(2)	La prise en charge des licences à durée limitée a été introduite.
Augmentation du nombre de VLAN pour l'ASA 5580	8.1(2)	Le nombre de VLAN pris en charge sur l'ASA 5580 est passé de 100 à 250.
Licence de sessions de mandataire pour les communications unifiées	8.0(4)	La licence de sessions de mandataire UC a été introduite. Les applications de mandataire téléphonique, de mandataire de fédération de présence et d'inspection de voix chiffrée utilisent des sessions de mandataire TLS pour leurs connexions. Chaque session de mandataire TLS est prise en compte dans la limite de licences UC. Toutes ces applications sont sous licence dans le cadre de l'offre de mandataires UC, et peuvent être combinées entre elles. Cette fonctionnalité n'est pas disponible dans la version 8.1.
Licence de filtre de trafic de réseau de zombies	8.2(1)	La licence de filtre de trafic de réseau de zombies a été introduite. Le filtre de trafic de réseau de zombies protège contre les activités réseau de programmes malveillants en suivant les connexions aux domaines et aux adresses IP connus pour être malveillants.

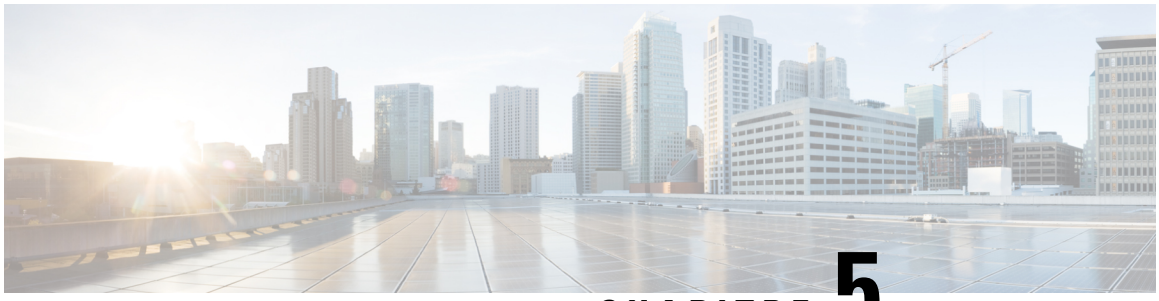
Nom de la caractéristique	Versions de plateforme	Description
Licence AnyConnect Essentials	8.2(1)	La licence AnyConnect Essentials a été introduite. Cette licence active l'accès client VPN AnyConnect à l'ASA. Cette licence ne prend pas en charge l'accès SSL VPN par navigateur ou Cisco Secure Desktop. Pour ces fonctionnalités, activez une licence AnyConnect Premium au lieu de la licence AnyConnect Essentials. **Remarque** Grâce à la licence AnyConnect Essentials, les utilisateurs de VPN peuvent utiliser un navigateur pour se connecter, télécharger et lancer (WebLaunch) le Secure Client (services client sécurisés). Le logiciel Secure Client (services client sécurisés) offre le même ensemble de fonctionnalités client, qu'il soit activé par cette licence ou une licence AnyConnect Premium. La licence AnyConnect Essentials ne peut pas être active en même temps que les licences suivantes sur un ASA donné : licence AnyConnect Premium (tous les types) ou licence d'évaluation de point d'accès avancée. Vous pouvez toutefois exécuter les licences AnyConnect Essentials et AnyConnect Premium sur différents ASA dans le même réseau. Par défaut, l'ASA utilise la licence AnyConnect Essentials, mais vous pouvez la désactiver pour utiliser d'autres licences en utilisant l'argument le volet Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau (client)) > Advanced (Avancé) > AnyConnect Essentials.
Licence SSL VPN remplacée par une licence AnyConnect Premium SSL VPN Edition	8.2(1)	Le nom de la licence SSL VPN a été remplacé par la licence AnyConnect Premium SSL VPN Edition.
Licences partagées pour SSL VPN	8.2(1)	Des licences partagées pour SSL VPN ont été introduites. Plusieurs ASA peuvent partager un ensemble de sessions SSL VPN selon les besoins.
L'application du mandataire de mobilité ne nécessite plus de licence de mandataire de connexions unifiées	8.2(2)	Le mandataire de mobilité ne nécessite plus la licence de mandataire UC.
Licence d'E/S 10 GE pour l'ASA 5585-X avec SSP-20	8.2(3)	Nous avons introduit la licence d'E/S 10 GE pour l'ASA 5585-X avec SSP-20 afin de permettre des vitesses de 10 Gigabit Ethernet pour les ports de fibre optique. Le SSP-60 prend en charge des vitesses de 10 Gigabit Ethernet par défaut. **Remarque** L'ASA 5585-X n'est pas pris en charge dans la version 8.3(x).

Nom de la caractéristique	Versions de plateforme	Description
Licence d'E/S 10 GE pour l'ASA 5585-X avec SSP-10	8.2(4)	Nous avons introduit la licence d'E/S 10 GE pour l'ASA 5585-X avec SSP-10 afin de permettre des vitesses de 10 Gigabit Ethernet pour les ports de fibre optique. Le SSP-40 prend en charge des vitesses de 10 Gigabit Ethernet par défaut. **Remarque** L'ASA 5585-X n'est pas pris en charge dans la version 8.3(x).
Licences de basculement non identiques	8.3(1)	Les licences de basculement n'ont plus besoin d'être identiques sur chaque unité. La licence utilisée pour les deux unités est la licence combinée des unités principale et secondaire. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Activation Key (Clé d'activation).
Licences empilables à durée limitée	8.3(1)	Les licences à durée limitée sont maintenant empilables. Dans de nombreux cas, vous devrez peut-être renouveler votre licence temporaire et effectuer une transition transparente de l'ancienne licence à la nouvelle. Pour les fonctionnalités qui ne sont disponibles qu'avec une licence à durée limitée, il est particulièrement important que la licence n'expire pas avant que vous puissiez appliquer la nouvelle licence. L'ASA vous permet d'*empiler* des licences à durée limitée afin que vous n'ayez pas à vous soucier de l'expiration de la licence ou de la perte de temps sur vos licences en raison de l'installation de la nouvelle licence plus tôt.
Licence Intercompany Media Engine	8.3(1)	La licence IME a été introduite.
Plusieurs licences à durée limitée actives en même temps	8.3(1)	Vous pouvez maintenant installer plusieurs licences à durée limitée et avoir une licence par fonctionnalité active à la fois. L'écran suivant a été modifié : Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Activation Key (Clé d'activation).
Activation et désactivation discrétionnaires des licences à durée limitée.	8.3(1)	Vous pouvez maintenant activer ou désactiver des licences à durée limitée à l'aide d'une commande. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Activation Key (Clé d'activation).
Licence AnyConnect Premium SSL VPN Edition remplacée par une licence AnyConnect Premium SSL VPN	8.3(1)	Le nom de la licence AnyConnect Premium SSL VPN Edition a été remplacé par la licence AnyConnect Premium SSL VPN.

Nom de la caractéristique	Versions de plateforme	Description
Aucune image de chiffrement des données utiles à exporter	8.3(2)	Si vous installez le logiciel sans chiffrement des données utiles sur les ASA 5505 à 5550, vous désactiverez les communications unifiées, le VPN de cryptage renforcé et les protocoles de gestion de cryptage renforcé. **Remarque** Cette image spéciale n'est prise en charge que dans 8.3(x); pour la prise en charge du chiffrement des données utiles dans les versions 8.4(1) et ultérieures, vous devez acheter une version matérielle spéciale de l'ASA.
Augmentation du nombre de contextes pour les ASA 5550, 5580 et 5585-X	v 8.4(1)	Pour les ASA 5550 et ASA 5585-X avec SSP-10, le nombre maximum de contextes est passé de 50 à 100. Pour les ASA 5580 et 5585-X avec SSP-20 et versions ultérieures, le maximum est passé de 50 à 250.
Augmentation du nombre de VLAN pour les ASA 5580 et 5585-X	v 8.4(1)	Pour les ASA 5580 et 5585-X, le nombre maximum de VLAN est passé de 250 à 1 024.
Augmentation du nombre de connexions pour les ASA 5580 et 5585-X	v 8.4(1)	Nous avons augmenté les limites de connexion du pare-feu : • ASA 5580-20 : 1 000 000 à 2 000 000. • ASA 5580-40 : 2 000 000 à 4 000 000. • ASA 5585-X avec SSP-10 : 750 000 à 1 000 000. • ASA 5585-X avec SSP-20 : 1 000 000 à 2 000 000. • ASA 5585-X avec SSP-40 : 2 000 000 à 4 000 000. • ASA 5585-X avec SSP-60 : 2 000 000 à 10 000 000.
Licence AnyConnect Premium SSL VPN remplacée par la licence AnyConnect Premium	v 8.4(1)	Le nom de la licence AnyConnect Premium SSL VPN a été remplacé par la licence AnyConnect Premium. L'affichage des renseignements sur la licence est passé de « SSL VPN Peers » (Homologues SSL VPN) à « AnyConnect Premium Peers » (Homologues AnyConnect Premium).
Augmentation du nombre de sessions VPN AnyConnect pour l'ASA 5580	v 8.4(1)	La limite de sessions VPN AnyConnect est passée de 5 000 à 10 000.
Augmentation du nombre de sessions Autre VPN pour l'ASA 5580	v 8.4(1)	La limite de sessions Autre VPN est passée de 5 000 à 10 000.

Nom de la caractéristique	Versions de plateforme	Description
VPN d'accès à distance IPsec avec IKEv2	v 8.4(1)	Le VPN d'accès à distance IPsec avec IKEv2 a été ajouté aux licences AnyConnect Essentials et AnyConnect Premium. **Remarque** La limite suivante existe dans notre prise en charge de IKEv2 sur l'ASA : nous ne prenons actuellement pas en charge les associations de sécurité en double. Les sessions de site à site IKEv2 ont été ajoutées à la licence Autre VPN (anciennement VPN IPsec). La licence Autre VPN est incluse dans la licence de base.
Aucun matériel de chiffrement des données utiles à exporter	v 8.4(1)	Pour les modèles disponibles sans chiffrement des données utiles (par exemple, l'ASA 5585-X), le logiciel ASA désactive les communications unifiées et les fonctions VPN, ce qui rend l'ASA disponible pour l'exportation vers certains pays.
Doubles SSP pour SSP-20 et SSP-40	8.4(2)	Pour SSP-40 et SSP-60, vous pouvez utiliser deux SSP de même niveau dans le même châssis. Les SSP de niveau mixte ne sont pas pris en charge (par exemple, un SSP-40 avec un SSP-60 n'est pas pris en charge). Chaque SSP agit en tant qu'appareil indépendant, avec des configurations et une gestion distinctes. Vous pouvez utiliser les deux SSP comme paire de basculement si vous le souhaitez. Lors de l'utilisation de deux SSP dans le châssis, le VPN n'est pas pris en charge; notez, cependant, que le VPN n'a pas été désactivé.
Licence de module IPS pour les modèles ASA 5512-X à ASA 5555-X	8.6(1)	Le module logiciel IPS SSP sur les modèles ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X et ASA 5555-X nécessite la licence de module IPS.
Licence de mise en grappe pour les modèles ASA 5580 et ASA 5585-X.	9.0(1)	Une licence de mise en grappe a été ajoutée pour les modèles ASA 5580 et ASA 5585-X.
Prise en charge du VPN sur l'ASASM	9.0(1)	L'ASASM prend désormais en charge toutes les fonctionnalités VPN.
Prise en charge des communications unifiées sur l'ASASM	9.0(1)	L'ASASM prend désormais en charge toutes les fonctionnalités de communications unifiées.
Prise en charge du double SSP ASA 5585-X pour les SSP-10 et SSP-20 (en plus de SSP-40 et SSP-60); prise en charge du VPN pour les doubles SSP	9.0(1)	L'ASA 5585-X prend désormais en charge les doubles SSP utilisant tous les modèles SSP (vous pouvez utiliser deux SSP de même niveau dans le même châssis). Le VPN est désormais pris en charge lors de l'utilisation de deux SSP.
Prise en charge de l'ASA 5500-X pour la mise en grappe	9.1(4)	Les modèles ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X et ASA 5555-X prennent désormais en charge les grappes de deux unités. La mise en grappe pour 2 unités est activée par défaut dans la licence de base; pour l'ASA 5512-X, vous avez besoin de la licence Security Plus.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de 16 membres d'une grappe pour l'ASA 5585-X	9.2(1)	L'ASA 5585-X prend désormais en charge les grappes de 16 unités.
Les licences des modèles ASAv4 et ASAv30 Standard et Premium ont été introduites	9.2(1)	L'ASAv a été introduit avec un schéma de licence simple : des licences permanentes ASAv4 et ASAv30 de niveau Standard ou Premium. Aucune licence complémentaire n'est disponible.



CHAPITRE 5

Licences : gestion des licences logicielles Smart

Smart Software Licensing vous permet d'acheter et de gérer un ensemble de licences de manière centralisée. Contrairement aux licences de clé d'autorisation de produit (PAK), les licences Smart ne sont pas liées à un numéro de série spécifique. Vous pouvez facilement déployer ou retirer des ASA sans avoir à gérer la clé de licence de chaque unité. Smart Software Licensing vous permet également de consulter votre utilisation et vos besoins en licences en un clin d'œil.

Remarque Smart Software Licensing n'est pas pris en charge sur ISA 3000. Ils utilisent des licences PAK. Consultez À propos des licences PAK, à la page 93.

Pour en savoir plus sur les fonctionnalités des licences Smart et les comportements par plateforme, consultez la section Gammes de produits compatibles avec les licences intelligentes.

- À propos des licences logicielles Smart, à la page 125
- Conditions préalables à la gestion de licences logicielles Smart, à la page 147
- Gestion des licences logicielles Smart, à la page 148
- Paramètres par défaut des licences logicielles Smart, à la page 149
- ASA virtuel : configurer les licences logicielles Smart, à la page 149
- Firepower 4100/9300 : configuration de la licence logicielle Smart, à la page 163
- Autres modèles : configurer les licences logicielles Smart, à la page 164
- Licences par modèle, à la page 178
- Supervision des licences logicielles Smart, à la page 190
- Communication avec Smart Software Manager, à la page 191
- Historique des licences logicielles Smart, à la page 194

À propos des licences logicielles Smart

Cisco Smart Licensing est un modèle de licence flexible qui vous offre un moyen plus facile, plus rapide et plus cohérent d'acheter et de gérer les logiciels du portefeuille Cisco et de votre organisme. De plus, il est sécurisé : vous contrôlez ce à quoi les utilisateurs peuvent accéder. Avec les licences Smart, vous obtenez :

- **Easy Activation** (Activation facile) : les licences Smart établissent un ensemble de licences logicielles qui peuvent être utilisées dans l'ensemble de l'entreprise. Plus de clés d'activation de produit (PAK).

- **Gestion unifiée** : Cisco License Central offre une vue complète de tous vos produits et services Cisco dans un portail facile à utiliser, afin que vous sachiez toujours ce que vous possédez et ce que vous utilisez.
- **License Flexibility** (Flexibilité des licences) : votre licence n'est pas verrouillée par un nœud sur votre matériel, vous pouvez donc facilement utiliser et transférer des licences selon vos besoins.

Pour utiliser les licences intelligentes, vous devez d'abord configurer un compte Smart sur Cisco License Central.

Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à Licensing Hub.

Licences logicielles Smart pour l'ASA sur le Châssis Firepower 4100/9300

Pour l'ASA sur le Châssis Firepower 4100/9300 , la configuration de la licence logicielle Smart est partagée entre le superviseur Châssis Firepower 4100/9300 et l'ASA.

- Châssis Firepower 4100/9300 : configurez toute l'infrastructure de licences logicielles Smart sur le châssis, y compris les paramètres de communication avec le Smart Software Manager. Le Châssis Firepower 4100/9300 lui-même ne nécessite aucune licence pour fonctionner. Consultez le guide de configuration FXOS pour connaître les procédures de licence.

Remarque La mise en grappe inter-châssis exige que vous activiez la même méthode de licence Smart sur chaque châssis de la grappe.

- Application ASA : configurez tous les droits de licence de l'ASA.

Gestionnaire de logiciels et comptes Smart

Lorsque vous achetez une ou plusieurs licences pour l'appareil, vous les gérez dans le Cisco Smart Software Manager :

https://software.cisco.com/#module/SmartLicensing

Smart Software Manager vous permet de créer un compte principal pour votre organisation.

Remarque Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.

Par défaut, vos licences sont affectées au *compte virtuel par défaut* sous votre compte maître. En tant qu'administrateur du compte, vous pouvez éventuellement créer des comptes virtuels supplémentaires; par exemple, vous pouvez créer des comptes pour des régions, les services ou les filiales. Plusieurs comptes virtuels vous permettent de gérer plus facilement un grand nombre de licences et de périphériques.

Gestion hors ligne

Si vos périphériques n'ont pas d'accès Internet et ne peuvent pas s'inscrire auprès du Smart Software Manager, vous devez configurer la licence hors ligne.

Réservation de licence permanente

Si vos périphériques ne peuvent pas accéder à Internet pour des raisons de sécurité, vous pouvez éventuellement demander des licences permanentes pour chaque ASA. Les licences permanentes ne nécessitent pas d'accès périodique à Smart Software Manager. Comme pour les licences PAK, vous pouvez acheter une licence et installer la clé de licence pour l'ASA. Contrairement à une licence PAK, vous pouvez obtenir et gérer les licences avec Smart Software Manager. Vous pouvez facilement passer du mode de licence Smart normal au mode de réservation de licence permanente.

Remarque L'ASA ne prend pas en charge la réservation d'une licence spécifique (SLR). Dans SLR, les droits de fonctionnalités spécifiques sont activés en permanence. L'ASA prend en charge uniquement le PLR, où toutes les fonctionnalités sont activées en permanence.

Réservation de licence permanente pour l'ASA virtuel

Remarque La réservation de licence permanente est prise en charge uniquement sur VMware et KVM.

Vous pouvez obtenir une licence spécifique au modèle qui active toutes les fonctionnalités suivantes :

- Débit maximal pour votre modèle
- Niveau Essentials
- Licence de cryptage renforcé (3DES et AES), si vous l'avez activée dans votre compte de licences Smart
- Fonctionnalités Secure Client (services client sécurisés) activées pour la plateforme

Remarque L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 133).

Mode de réservation de licences permanentes en fonction de la mémoire et du vCPU

Vous pouvez configurer une licence spécifique au modèle en fonction de la RAM et des vCPU attribuées à votre ASA virtuel. Par exemple, un ASA virtuel avec 8 Go de RAM et 4 vCPU utilise toujours une licence ASAv30 avec un débit de 2 Go.

Les relations entre les vCPU et la mémoire à la licence sont les suivantes :

- 2 Go, 1 vCPU – ASAv5 (100 M) (Vous devez exécuter la commande **license smart set_plr5**; sinon, la licence ASAv10 est attribuée pour autoriser un débit de 1 Go.)

Remarque Dans la version 9.13, les exigences de RAM ASAv5 ont été augmentées à 2 Go. En raison de cette augmentation, la licence permanente ASAv5 ne fonctionnait plus, car l'ASA vérifiait la mémoire attribuée et déterminait que 2 Go de RAM correspondaient en réalité à une licence ASAv10, et non ASAv5. Pour permettre à la licence permanente ASAv5 de fonctionner, vous devez configurer l'ASA afin qu'il reconnaisse la mémoire supplémentaire pour le modèle.

- 2 Go, 1 vCPU – ASAv10 (1G)
- 8 Go, 4 vCPU – ASAv30 (2G)
- 16 Go, 8 vCPU – ASAv50 (10G)
- 32 Go, 16 vCPU – ASAv100 (20G)

Plus tard, si vous souhaitez modifier le niveau de modèle d'une unité, vous devrez renvoyer la licence actuelle et demander une nouvelle licence au niveau de modèle correct. Pour modifier le modèle d'un ASA virtuel déjà déployé, à partir de l'hyperviseur, vous pouvez modifier les paramètres des vCPU et de la DRAM pour qu'ils correspondent aux exigences du nouveau modèle. Consultez le *Guide de démarrage d'ASA virtuel virtuel* pour connaître ces valeurs.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA virtuel, puis saisir ce code dans Smart Software Manager. Vous devez suivre correctement le processus de retour pour vous assurer de ne pas payer pour les licences inutilisées.

Pour en savoir plus sur la configuration de la réservation de licence permanente, consultez ASA virtuel: configurer la réservation de licence permanente, à la page 159.

Réservation de licence permanente pour Firepower 1010

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Security Plus
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 133).

Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour Firepower 1100

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Nombre maximum de contextes de sécurité
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 133).



Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour Firepower 2100

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Nombre maximum de contextes de sécurité
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 133).



Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour Secure Firewall 3100

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Nombre maximum de contextes de sécurité
- Licence d'opérateur
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 133).



Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour le châssis Firepower 4100/9300

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials.
- Nombre maximum de contextes de sécurité
- Licence d'opérateur
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 133).



Remarque La licence est gérée sur le Châssis Firepower 4100/9300 , mais vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation. Pour gérer la licence, consultez le Guide de configuration FXOS.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur le Châssis Firepower 4100/9300 , puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Smart Software Manager sur place

Si vos périphériques ne peuvent pas accéder à Internet pour des raisons de sécurité, vous pouvez éventuellement installer un serveur Smart Software Manager sur site (anciennement appelé « serveur satelitte Smart Software ») local en tant que machine virtuelle (VM). Smart Software Manager sur site fournit un sous-ensemble des fonctionnalités de Smart Software Manager et vous permet de fournir des services de licence essentiels pour tous vos périphériques locaux. Seul Smart Software Manager sur site doit se connecter périodiquement au Smart Software Manager principal pour synchroniser votre utilisation des licences. Vous pouvez effectuer la synchronisation selon un calendrier défini ou manuellement.

Vous pouvez exécuter les fonctions suivantes sur Smart Software Manager sur site :

- Activer ou enregistrer une licence
- Afficher les licences de votre entreprise
- Transférer des licences entre les entités de l'entreprise

Pour en savoir plus, consultez la Fiche technique de Cisco Smart Software Manager sur site.

Licences et appareils gérés par compte virtuel

Les licences et les périphériques sont gérés par compte virtuel : seuls les périphériques de ce compte virtuel peuvent utiliser les licences attribuées au compte. Si vous avez besoin de licences supplémentaires, vous pouvez transférer une licence inutilisée d'un autre compte virtuel. Vous pouvez également transférer des périphériques entre des comptes virtuels.

Pour l'ASA sur le Châssis Firepower 4100/9300 :seul le châssis s'enregistre en tant que périphérique, tandis que les applications ASA dans le châssis demandent leurs propres licences. Par exemple, pour un châssis Firepower 9300 avec 3 modules de sécurité, le châssis compte comme un seul périphérique, mais les modules utilisent 3 licences distinctes.

Licence d'évaluation.

ASA virtuel

L'ASA virtuel ne prend pas en charge de mode d'évaluation. Avant que l'ASA virtuel ne s'enregistre avec Smart Software Manager, il fonctionne dans un état fortement limité en termes de débit.

Firepower 1000

Avant que le Firepower 1000 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. Seuls les droits par défaut sont activés. À la fin de cette période, le Firepower 1000 devient non conforme.

Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

Firepower de la série 2100

Avant que le Firepower 2100 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. Seuls les droits par défaut sont activés. À la fin de cette période, le Firepower 2100 devient non conforme.



Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

Cisco Secure Firewall 3100

Avant que le Secure Firewall 3100 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. Seuls les droits par défaut sont activés. À la fin de cette période, le Secure Firewall 3100 devient non conforme.



Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

Châssis Firepower 4100/9300

Le Châssis Firepower 4100/9300 prend en charge deux types de licence d'évaluation :

- Mode d'évaluation au niveau du châssis : avant que le Châssis Firepower 4100/9300 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. L'ASA ne peut pas demander de droits spécifiques dans ce mode; seuls les droits par défaut sont activés. À la fin de cette période, le Châssis Firepower 4100/9300 devient non conforme.
- Mode d'évaluation basé sur les droits : après l'enregistrement de Châssis Firepower 4100/9300 auprès de Smart Software Manager, vous pouvez obtenir des licences d'évaluation à durée limitée qui peuvent être attribuées à l'ASA. Dans l'ASA, vous demandez des droits comme d'habitude. Lorsque la licence à durée limitée expire, vous devez soit renouveler la licence à durée limitée, soit obtenir une licence permanente.



Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager et obtenir une licence permanente pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

À propos des licences par type

Les sections suivantes contiennent des renseignements supplémentaires sur les licences par type.

LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement

Les licences Secure Client (services client sécurisés) ne sont pas appliquées directement à l'ASA. Cependant, vous devez acheter des licences et les ajouter à votre compte Smart pour garantir le droit d'utiliser l'ASA comme tête de réseau Secure Client (services client sécurisés).

- Pour les licences Secure Client Advantage et Secure Client Premier, ajoutez le nombre d'homologues que vous envisagez d'utiliser pour tous les ASA de votre compte Smart et achetez des licences pour ce nombre d'homologues.
- Pour le VPN client sécurisé uniquement , achetez une licence par ASA. Contrairement aux autres licences qui fournissent un ensemble d'homologues pouvant être partagés par plusieurs ASA, la licence VPN client sécurisé uniquement est gérée par tête de réseau.

Pour obtenir plus de renseignements, consultez la section :

- Guide de commande Cisco Secure Client (services client sécurisés)
- Foire aux questions (FAQ) Secure Client (services client sécurisés) Licensing

Autres homologues VPN

Les autres homologues VPN comprennent les types de VPN suivants :

- VPN d'accès à distance IPsec avec IKEv1
- VPN de site à site IPsec avec IKEv1
- VPN de site à site IPsec avec IKEv2

Cette licence est incluse dans la licence de base.

Total des homologues VPN combinés, tous types

- Le nombre total d'homologues VPN est le nombre maximum d'homologues VPN autorisés pour les homologues Secure Client (services client sécurisés) et autres homologues VPN combinés. Par exemple, si le total est de 1 000, vous pouvez autoriser 500 homologues Secure Client (services client sécurisés) et 500 autres homologues VPN simultanément; ou 700 homologues Secure Client (services client sécurisés) et 300 autres VPN; ou utiliser les 1 000 pour Secure Client (services client sécurisés). Si vous dépassez le nombre total d'homologues VPN, vous pouvez surcharger l'ASA. Assurez-vous donc de dimensionner votre réseau de manière appropriée.

Licence de chiffrement

Cryptage renforcé : ASA virtuel

Le cryptage renforcé (3DES/AES) est disponible pour les connexions de gestion avant de vous connecter au Smart Software Manager ou au serveur Smart Software Manager sur site afin que vous puissiez lancer ASDM et vous connecter au Smart Software Manager. Pour le trafic de transit qui nécessite un cryptage renforcé (comme VPN), le débit est fortement limité jusqu'à ce que vous vous connectiez à Smart Software Manager et obteniez la licence de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour l'ASA virtuel à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered**

with this token (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation). Si l'ASA virtuel devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA virtuel conservera la licence et ne reviendra pas à l'état de débit limité. La licence est supprimée si vous réenregistrez l'ASA virtuel et que la conformité à l'exportation est désactivée, ou si vous restaurez les paramètres d'usine par défaut de l'ASA virtuel.

Si vous enregistrez initialement l'ASA virtuel sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'ASA virtuel pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

Cryptage renforcé : Firepower 1000, Firepower 2100 en mode appareil, Secure Firewall 3100

L'ASA inclut la capacité 3DES par défaut pour l'accès de gestion uniquement, de sorte que vous pouvez vous connecter au gestionnaire de logiciels intelligents et utiliser ASDM immédiatement. Vous pouvez également utiliser SSH et SCP si vous configurez ultérieurement l'accès SSH sur l'ASA. D'autres fonctions qui nécessitent un cryptage renforcé (comme le VPN) doivent avoir le cryptage renforcé activé, ce qui exige que vous vous inscriviez d'abord au Smart Software Manager.



Remarque Si vous tentez de configurer des fonctions pouvant utiliser un cryptage renforcé avant de vous inscrire - même si vous ne configurez qu'un cryptage faible - votre connexion HTTPS sera interrompue sur cette interface, et vous ne pourrez pas vous reconnecter. Il y a une exception à cette règle si vous êtes connecté à une interface de gestion uniquement, telle que Management 1/1. SSH n'est pas affecté. Si vous perdez votre connexion HTTPS, vous pouvez vous connecter au port de console pour reconfigurer l'ASA, vous connecter à une interface de gestion uniquement, ou vous connecter à une interface non configurée pour une fonction de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour l'ASA à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation). Si l'ASA devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA continuera d'autoriser le trafic de transit. Même si vous réenregistrez l'ASA et que la conformité à l'exportation est désactivée, la licence reste activée. La licence est supprimée si vous restaurez l'ASA aux paramètres d'usine par défaut.

Si vous enregistrez initialement l'ASA sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'ASA pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

Remarque Le rechargement d'un périphérique avec un enregistrement de licence expiré depuis plus d'un an désactivera la fonctionnalité contrôlée à l'exportation. Cela peut entraîner des problèmes critiques tels qu'une interruption du VPN ou des scénarios de basculement « split brain » lorsque le chiffrement IPsec est activé.

Cryptage renforcé : Firepower 2100 en mode plateforme

Le cryptage renforcé (3DES/AES) est disponible pour les connexions de gestion avant de vous connecter au Smart Software Manager ou au serveur Smart Software Manager sur site afin que vous puissiez lancer ASDM. Notez que l'accès ASDM est disponible sur les interfaces de gestion uniquement avec le chiffrement par défaut. Le trafic de transit qui nécessite un cryptage renforcé (comme VPN) n'est pas autorisé jusqu'à ce que vous vous connectiez et obteniez la licence de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour l'ASA à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation). Si l'ASA devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA continuera d'autoriser le trafic de transit. Même si vous réenregistrez l'ASA et que la conformité à l'exportation est désactivée, la licence reste activée. La licence est supprimée si vous restaurez l'ASA aux paramètres d'usine par défaut.

Si vous enregistrez initialement l'ASA sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'ASA pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

Cryptage renforcé : Châssis Firepower 4100/9300

Lorsque l'ASA est déployé en tant que périphérique logique, vous pouvez lancer ASDM immédiatement. Le trafic de transit qui nécessite un cryptage renforcé (comme VPN) n'est pas autorisé jusqu'à ce que vous vous connectiez et obteniez la licence de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour le châssis à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation).

Si l'ASA devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA continuera d'autoriser le trafic de transit. La licence est supprimée si vous réenregistrez le châssis et que la conformité à l'exportation est désactivée, ou si vous restaurez les paramètres d'usine par défaut du châssis.

Si vous enregistrez initialement le châssis sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'application ASA pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

DES : tous les modèles

Si le cryptage renforcé est activé, vous ne pouvez pas utiliser DES.

Licence d'opérateur

La licence d'opérateur permet d'utiliser les fonctionnalités d'inspection suivantes :

- Diameter : Diameter est un protocole d'authentification, d'autorisation et de comptabilité (AAA) utilisé dans les réseaux de télécommunications fixes et mobiles de nouvelle génération tels que SPE (Evolved Packet System) pour LTE (Long Term Évolution) et IMS (IP Multimédia Subsystem). Il remplace RADIUS et TACACS dans ces réseaux.
- GTP/GPRS : le protocole de tunnellisation GPRS est utilisé dans les réseaux SMS, UMTS et LTE pour le trafic du service radio général par paquets (GPRS). GTP fournit un protocole de gestion et de contrôle de tunnel pour fournir un accès réseau GPRS à une station mobile par la création, la modification et la suppression de tunnels. GTP utilise également un mécanisme de tunnellisation pour acheminer les paquets de données des utilisateurs.
- M3UA : MTP3 User Adaptation (M3UA) est un protocole client/serveur qui fournit une passerelle vers le réseau SS7 pour les applications IP qui communiquent avec la couche MTP3 (Message Transfer Part 3) de SS7. M3UA permet d'exécuter les composants SS7 (comme ISUP) sur un réseau IP. M3UA est défini dans la RFC 4666.
- SCTP : le protocole SCTP (Stream Control Transmission Protocol) est décrit dans la RFC 4960. Le protocole prend en charge le protocole de signalisation téléphonique SS7 sur IP et est également un protocole de transport pour plusieurs interfaces dans l'architecture de réseau mobile LTE 4G.

Nombre total de sessions de mandataire TLS

Chaque session de mandataire TLS pour l'inspection vocale chiffrée est prise en compte dans la limite de licences TLS.

D'autres applications qui utilisent des sessions de mandataire TLS ne sont pas prises en compte dans la limite du TLS, par exemple, le mandataire Mobility Advantage (qui ne nécessite pas de licence).

Certaines applications peuvent utiliser plusieurs sessions pour une connexion. Par exemple, si vous configurez un téléphone avec un Cisco Unified Communications Manager principal et de secours, il y a 2 connexions de mandataire TLS.

Vous définissez indépendamment la limite de mandataire TLS à l'aide de la commande **tls-proxy maximum-sessions** ou dans ASDM, en utilisant le volet **Configuration > Firewall (Pare-feu) > Unified Communications (Communications unifiées) > TLS Proxy (Mandataire TLS)**. Pour afficher les limites de votre modèle, saisissez la commande **tls-proxy maximum-sessions ?**. Lorsque vous appliquez une licence de mandataire TLS supérieure à la limite de mandataire TLS par défaut, l'ASA définit automatiquement la limite de mandataire TLS pour correspondre à la licence. La limite de mandataire TLS a priorité sur la limite de la licence; si vous définissez la limite de mandataire TLS pour qu'elle soit inférieure à la licence, vous ne pouvez pas utiliser toutes les sessions de votre licence.

Remarque Pour les licences dont la référence se termine par « K8 » (par exemple, les licences de moins de 250 utilisateurs), les sessions de mandataire TLS sont limitées à 1 000. Pour les licences dont la référence se termine par « K9 » (par exemple, les licences de 250 utilisateurs ou plus), la limite de mandataire TLS dépend de la configuration, jusqu'à la limite du modèle. K8 et K9 indiquent si la licence est restreinte pour l'exportation : la licence K8 n'est pas limitée tandis que la licence K9 est restreinte.

Si vous effacez la configuration (à l'aide de la commande **clear configure all**, par exemple), la limite de mandataire TLS est définie par défaut pour votre modèle; si cette valeur par défaut est inférieure à la limite de licence, vous verrez un message d'erreur pour utiliser la commande **tls-proxy maximum-sessions** afin d'augmenter à nouveau la limite (dans ASDM, utilisez le volet **TLS Proxy** (Mandataire TLS)). Si vous utilisez le basculement et saisissez la commande **write standby** ou dans ASDM, utilisez **File (Fichier) > Save Running Configuration to Standby Unit (Enregistrer la configuration d'exécution sur l'unité en veille)** sur l'unité principale pour forcer une synchronisation de la configuration; la commande **clear configure all** est générée automatiquement sur l'unité secondaire, vous pouvez donc voir le message d'avertissement sur l'unité secondaire. Étant donné que la synchronisation de la configuration restaure la limite de mandataire TLS définie sur l'unité principale, vous pouvez ignorer l'avertissement.

Vous pouvez également utiliser des sessions de chiffrement SRTP pour vos connexions :

- Pour les licences K8, les sessions SRTP sont limitées à 250.
- Pour les licences K9, il n'y a pas de limite.

Remarque Seuls les appels qui nécessitent un chiffrement ou un déchiffrement pour un support sont pris en compte dans la limite du SRTP; si la transmission est définie pour l'appel, même si les deux segments sont des SRTP, ils ne sont pas pris en compte dans la limite.

Nombre maximum de VLAN

Pour qu'une interface soit prise en compte dans la limite de VLAN, vous devez lui attribuer un VLAN.

Licence de filtre de trafic de réseau de zombies

Nécessite une licence de cryptage renforcé (3DES/AES) pour télécharger la base de données dynamique.

Licences de basculement ou de grappe ASA

Licences de basculement pour l'ASAv

L'unité en veille requiert le même modèle de licence que l'unité principale.

Licences de basculement pour Firepower 1010

Smart Software Manager standard et sur site

Les deux unités Firepower 1010 doivent être enregistrées auprès du serveur Smart Software Manager ou du Smart Software Manager sur site. Les deux unités nécessitent que vous activiez la licence Essentials et la licence Security Plus *avant* de pouvoir configurer le basculement.

En règle générale, vous n'avez pas également besoin d'activer la licence de fonction de cryptage renforcé (3DES/AES) dans l'ASA, car les deux unités devraient avoir obtenu le jeton de cryptage renforcé lorsque vous avez enregistré les unités. Lors de l'utilisation du jeton d'enregistrement, les deux unités doivent avoir le même niveau de chiffrement.

Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Dans ce cas, activez-la sur l'unité active après avoir activé le basculement. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. Seule l'unité active demande la licence au serveur. La licence est agrégée en une seule licence de basculement partagée par la paire de basculement, et cette licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement. Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce et que vous n'utilisez pas le jeton de cryptage renforcé, vous ne pourrez pas apporter de modifications de configuration aux fonctionnalités nécessitant la licence de fonctionnalité de cryptage renforcé (3DES/AES); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour Firepower 1100

Smart Software Manager standard et sur site

Seule l'unité active demande des licences auprès du serveur. Les licences sont agrégées en une seule licence de basculement partagée par la paire de basculement. Il n'y a pas de frais supplémentaires pour les unités secondaires.

Après avoir activé le basculement, pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. La licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement.

Remarque Chaque ASA doit avoir la même licence de chiffrement lors de la formation d'une paire de basculement. Lorsque vous enregistrez un ASA sur le serveur de licences Smart, la licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. En raison de cette exigence, vous avez deux choix de licence lorsque vous utilisez le jeton de cryptage renforcé avec le basculement:

- Avant d'activer le basculement, enregistrez les deux unités sur le serveur de licences smart. Dans ce cas, les deux unités auront un cryptage renforcé. Ensuite, après avoir activé le basculement, continuez de configurer les droits de licence sur l'unité active. Si vous activez le chiffrement pour la liaison de basculement, il utilisera AES/3DES (cryptage renforcé).
- Avant d'enregistrer l'unité active sur le serveur de licences smart, activez le basculement. Dans ce cas, les deux unités n'auront pas encore de cryptage renforcé. Configurez ensuite les droits de licence et enregistrez l'unité active sur le serveur de licences smart; les deux unités obtiendront un cryptage renforcé de la licence agrégée. Notez que si vous avez activé le chiffrement sur la liaison de basculement, il utilisera des DES (chiffrement faible), car la liaison de basculement a été établie avant que les unités n'acquièrent le cryptage renforcé. Vous devez recharger *les deux* unités pour utiliser AES/3DES sur la liaison. Si vous ne rechargez qu'une seule unité, cette unité tentera d'utiliser AES/ 3DES pendant que l'unité d'origine utilise DES, ce qui rendra active les deux unités (déconnexion cérébrale).

Chaque type de licence complémentaire est géré comme suit :

- Essentials : bien que seule l'unité active demande cette licence au serveur, l'unité en veille a la licence Essentials activée par défaut; elle n'a pas besoin de s'inscrire auprès du serveur pour l'utiliser.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 2 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 2 contextes; pour deux unités Firepower 1120, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 3 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 7 contextes. Cependant, comme la limite de plateformes pour une unité est de 5, la licence combinée autorise un maximum de 5 contextes uniquement. Dans ce cas, vous pourriez uniquement configurer la licence de contexte active pour 1 contexte.
  - Active/actif : la licence Essentials comprend 2 contextes; pour deux unités Firepower 1140, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 4 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 8 contextes. Une unité peut utiliser 5 contextes et l'autre unité peut utiliser 3 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 8. Comme la limite de plateformes pour une unité est de 10, la licence combinée autorise un maximum de 10 contextes; les 8 contextes sont dans la limite.
- Cryptage renforcé (3DES/AES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne

unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales (c.-à-d. ajouter un contexte supplémentaire); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour Firepower 2100

Smart Software Manager standard et sur site

Seule l'unité active demande des licences auprès du serveur. Les licences sont agrégées en une seule licence de basculement partagée par la paire de basculement. Il n'y a pas de frais supplémentaires pour les unités secondaires.

Après avoir activé le basculement, pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. La licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement.

Remarque Chaque ASA doit avoir la même licence de chiffrement lors de la formation d'une paire de basculement. Lorsque vous enregistrez un ASA sur le serveur de licences Smart, la licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. En raison de cette exigence, vous avez deux choix de licence lorsque vous utilisez le jeton de cryptage renforcé avec le basculement:

- Avant d'activer le basculement, enregistrez les deux unités sur le serveur de licences smart. Dans ce cas, les deux unités auront un cryptage renforcé. Ensuite, après avoir activé le basculement, continuez de configurer les droits de licence sur l'unité active. Si vous activez le chiffrement pour la liaison de basculement, il utilisera AES/3DES (cryptage renforcé).
- Avant d'enregistrer l'unité active sur le serveur de licences smart, activez le basculement. Dans ce cas, les deux unités n'auront pas encore de cryptage renforcé. Configurez ensuite les droits de licence et enregistrez l'unité active sur le serveur de licences smart; les deux unités obtiendront un cryptage renforcé de la licence agrégée. Notez que si vous avez activé le chiffrement sur la liaison de basculement, il utilisera des DES (chiffrement faible), car la liaison de basculement a été établie avant que les unités n'acquièrent le cryptage renforcé. Vous devez recharger *les deux* unités pour utiliser AES/3DES sur la liaison. Si vous ne rechargez qu'une seule unité, cette unité tentera d'utiliser AES/ 3DES pendant que l'unité d'origine utilise DES, ce qui rendra active les deux unités (déconnexion cérébrale).

Chaque type de licence complémentaire est géré comme suit :

- Essentials : bien que seule l'unité active demande cette licence au serveur, l'unité en veille a la licence Essentials activée par défaut; elle n'a pas besoin de s'inscrire auprès du serveur pour l'utiliser.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 2 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 2 contextes; pour deux unités Firepower 2130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 30 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 34 contextes. Cependant, comme la limite de plateformes pour une unité est de 30, la licence combinée autorise un maximum de 30 contextes uniquement. Dans ce cas, vous pourriez uniquement configurer la licence de contexte active pour 25 contextes.
  - Active/actif : la licence Essentials comprend 2 contextes; pour deux unités Firepower 2130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 10 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 14 contextes. Une unité peut utiliser 9 contextes et l'autre unité peut utiliser 5 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 14. Comme la limite de plateformes pour une unité est de 30, la licence combinée autorise un maximum de 30 contextes; les 14 contextes sont dans la limite.
- Cryptage renforcé (3DES/AES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales (c.-à-d. ajouter un contexte supplémentaire); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour Cisco Secure Firewall 3100

Smart Software Manager standard et sur site

Chaque unité requiert la licence Essentials (activée par défaut) et la même licence de chiffrement. Nous vous conseillons d'accorder une licence à chaque unité avec le serveur de licences *avant* d'activer le basculement pour éviter les problèmes de non-concordance de licences et, lors de l'utilisation de la licence de cryptage renforcé, des problèmes de chiffrement de la liaison de basculement.

La fonctionnalité de basculement elle-même ne nécessite aucune licence. Il n'y a pas de coût supplémentaire pour la licence de contexte sur les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, la licence Essentials est toujours activée par défaut sur les deux unités. Après avoir activé le basculement, pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. La licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement.

Chaque type de licence complémentaire est géré comme suit :

- Essentials : chaque unité demande une licence Essentials au serveur.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 2 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 2 contextes; pour deux unités Secure Firewall 3130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 100 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 104 contextes. Cependant, comme la limite de plateformes pour une unité est de 100, la licence combinée autorise un maximum de 100 contextes uniquement. Dans ce cas, vous pourriez uniquement configurer la licence de contexte active pour 95 contextes.
  - Active/active : la licence Essentials comprend 2 contextes; pour deux unités Secure Firewall 3130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 10 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 14 contextes. Une unité peut utiliser 9 contextes et l'autre unité peut utiliser 5 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 14. Comme la limite de plateformes pour une unité est de 100, la licence combinée autorise un maximum de 100 contextes; les 14 contextes sont dans la limite.
- Cryptage renforcé (3DES/AES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales (c.-à-d. ajouter un contexte supplémentaire); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état

mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour le Firepower 4100/9300

Smart Software Manager standard et sur site

Les deux Firepower 4100/9300 doivent être enregistrés auprès du Smart Software Manager ou du Smart Software Manager sur site avant de configurer le basculement. Il n'y a pas de frais supplémentaires pour les unités secondaires.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Lors de l'utilisation du jeton, chaque châssis doit avoir la même licence de chiffrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Après avoir activé le basculement, pour la configuration de la licence ASA pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. Seule l'unité active demande les licences auprès du serveur. Les licences sont agrégées en une seule licence de basculement partagée par la paire de basculement, et cette licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : bien que seule l'unité active demande cette licence au serveur, l'unité en veille a la licence Essentials activée par défaut; elle n'a pas besoin de s'inscrire auprès du serveur pour l'utiliser.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 10 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 10 contextes; pour 2 unités, ces licences ajoutent jusqu'à 20 contextes. Vous configurez une licence de 250 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 270 contextes. Cependant, comme la limite de plateformes pour une unité est de 250, la licence combinée autorise un maximum de 250 contextes uniquement. Dans ce cas, vous devez configurer uniquement la licence de contexte active pour 230 contextes.
  - Active/active : la licence Essentials comprend 10 contextes; pour 2 unités, ces licences ajoutent jusqu'à 20 contextes. Vous configurez une licence de 10 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 30 contextes. Une unité peut utiliser 17 contextes et l'autre unité peut utiliser 13 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 30. Comme la limite de plateformes pour une unité est de 250, la licence combinée autorise un maximum de 250 contextes; les 30 contextes sont dans la limite.
- Opérateur : seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

- Cryptage renforcé (3DES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de grappe ASA pour Cisco Secure Firewall 3100

Smart Software Manager standard et sur site

Chaque unité requiert la licence Essentials (activée par défaut) et la même licence de chiffrement. Nous vous conseillons d'accorder une licence à chaque unité avec le serveur de licences *avant* d'activer la mise en grappe pour éviter les problèmes de non-concordance de licences et, lors de l'utilisation de la licence de cryptage renforcé, des problèmes de chiffrement de la liaison de commande de grappe.

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence. Il n'y a pas de coût supplémentaire pour la licence de contexte sur les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, la licence Essentials est toujours activée par défaut sur toutes les unités. Vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : chaque unité demande une licence Essentials au serveur.
- Contexte : seule l'unité de contrôle demande la licence de contexte au serveur. La licence Essentials comprend 2 contextes par défaut et est présente sur tous les membres de la grappe. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité de contrôle, sont combinées jusqu'à la limite de plateformes dans une licence de grappe agrégée. Par exemple :
  - Vous avez 6 appareils Secure Firewall 3100 dans la grappe. La licence Essentials comprend 2 contextes; pour 6 unités, ces licences ajoutent jusqu'à 12 contextes. Vous configurez une licence de 20 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée

comprend 32 contextes. Comme la limite de plateformes pour un châssis est de 100, la licence combinée autorise un maximum de 100 contextes; les 32 contextes sont dans la limite. Par conséquent, vous pouvez configurer jusqu'à 32 contextes sur l'unité de contrôle; chaque unité de données aura également 32 contextes par la réplication de la configuration.

- Vous avez 3 appareils Secure Firewall 3100 dans la grappe. La licence Essentials comprend 2 contextes; pour 3 unités, ces licences ajoutent jusqu'à 6 contextes. Vous configurez une licence de 100 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 106 contextes. Comme la limite de plateformes pour une unité est de 100, la licence combinée autorise un maximum de 100 contextes; les 106 contextes sont au-dessus de la limite. Par conséquent, vous ne pouvez configurer que 100 contextes sur l'unité de contrôle; chaque unité de données aura également 100 contextes par la réplication de la configuration. Dans ce cas, vous devez uniquement configurer la licence de contexte de l'unité de contrôle pour 94 contextes.

- Cryptage renforcé (3DES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité de contrôle demande cette licence et toutes les unités peuvent l'utiliser en raison de l'agrégation des licences.

Si une nouvelle unité de contrôle est choisie, la nouvelle unité de contrôle continue d'utiliser la licence agrégée. Elle utilise également la configuration de licence mise en mémoire cache pour demander à nouveau la licence de l'unité de contrôle. Lorsque l'ancienne unité de contrôle rejoint la grappe en tant qu'unité de données, elle libère le droit de licence de l'unité de contrôle. Avant que l'unité de données ne libère la licence, la licence de l'unité de contrôle peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La licence conservée est valide pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Vous devez éviter de modifier la configuration jusqu'à ce que les demandes de licences soient complètement traitées. Si une unité quitte la grappe, la configuration de contrôle mise en mémoire cache est supprimée, tandis que les droits par unité sont conservés. En particulier, vous devrez demander à nouveau la licence de contexte sur les unités qui ne sont pas des grappes.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer la mise en grappe.

Licences de grappe ASA pour l'ASAv

Smart Software Manager standard et sur site

Chaque unité nécessite la même licence de débit et la même licence de chiffrement. Nous vous conseillons d'accorder une licence à chaque unité avec le serveur de licences *avant* d'activer la mise en grappe pour éviter les problèmes de non-concordance de licences et, lors de l'utilisation de la licence de cryptage renforcé, des problèmes de chiffrement de la liaison de commande de grappe.

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent

pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : seule l'unité de contrôle demande la licence Essentials au serveur et toutes les unités peuvent l'utiliser en raison de l'agrégation des licences.
- Débit : chaque unité demande sa propre licence de débit auprès du serveur.
- Cryptage renforcé (3DES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité de contrôle demande cette licence et toutes les unités peuvent l'utiliser en raison de l'agrégation des licences.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque unité et activer les licences *avant* de configurer la mise en grappe.

Licences de grappe ASA pour l'Firepower 4100/9300

Smart Software Manager standard et sur site

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence. Pour utiliser le cryptage renforcé et d'autres licences facultatives, chaque Châssis Firepower 4100/9300 doit être enregistré auprès de l'autorité de licence ou du serveur Smart Software Manager standard et sur site. Il n'y a pas de frais supplémentaires pour les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Lors de l'utilisation du jeton, chaque châssis doit avoir la même licence de chiffrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : seule l'unité de contrôle demande la licence Essentials au serveur et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.
- Contexte : seule l'unité de contrôle demande la licence de contexte au serveur. La licence Essentials comprend 10 contextes par défaut et est présente sur tous les membres de la grappe. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité de contrôle, sont combinées jusqu'à la limite de plateformes dans une licence de grappe agrégée. Par exemple :
  - Vous avez 6 modules Firepower 9300 dans la grappe. La licence Essentials comprend 10 contextes; pour 6 unités, ces licences ajoutent jusqu'à 60 contextes. Vous configurez une licence de 20 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 80 contextes. Comme la limite de plateformes pour un module est de 250, la licence combinée autorise un maximum de 250 contextes; les 80 contextes sont dans la limite. Par conséquent, vous pouvez configurer jusqu'à 80 contextes sur l'unité de contrôle; chaque unité de données aura également 80 contextes par la réplication de la configuration.

- Vous avez 3 unités Firepower 4112 dans la grappe. La licence Essentials comprend 10 contextes; pour 3 unités, ces licences ajoutent jusqu'à 30 contextes. Vous configurez une licence de 250 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 280 contextes. Comme la limite de plateformes pour une unité est de 250, la licence combinée autorise un maximum de 250 contextes; les 280 contextes sont au-dessus de la limite. Par conséquent, vous ne pouvez configurer que 250 contextes sur l'unité de contrôle; chaque unité de données aura également 250 contextes par la réplication de la configuration. Dans ce cas, vous devez uniquement configurer la licence de contexte de l'unité de contrôle pour 220 contextes.

- Opérateur : requis pour le VPN S2S distribué. Cette licence est un droit par unité, et chaque unité demande sa propre licence au serveur.
- Cryptage renforcé (3DES) : pour un déploiement Cisco Smart Software Manager sur site antérieur à la version 2.3.0, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Cette licence est un droit par unité, et chaque unité demande sa propre licence au serveur.

Si une nouvelle unité de contrôle est choisie, la nouvelle unité de contrôle continue d'utiliser la licence agrégée. Elle utilise également la configuration de licence mise en mémoire cache pour demander à nouveau la licence de l'unité de contrôle. Lorsque l'ancienne unité de contrôle rejoint la grappe en tant qu'unité de données, elle libère le droit de licence de l'unité de contrôle. Avant que l'unité de données ne libère la licence, la licence de l'unité de contrôle peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La licence conservée est valide pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement d'autorisation toutes les 12 heures jusqu'à ce que la licence soit conforme. Vous devez éviter de modifier la configuration jusqu'à ce que les demandes de licences soient complètement traitées. Si une unité quitte la grappe, la configuration de contrôle mise en mémoire cache est supprimée, tandis que les droits par unité sont conservés. En particulier, vous devrez demander à nouveau la licence de contexte sur les unités qui ne sont pas des grappes.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer la mise en grappe.

Conditions préalables à la gestion de licences logicielles Smart

Conditions préalables de Smart Software Manager standard et sur site

Firepower 4100/9300

Configurez l'infrastructure de licence logicielle Smart sur le Châssis Firepower 4100/9300 avant de configurer les droits de licence ASA.

Tous les autres modèles

- Assurez-vous de l'accès Internet, de l'accès au mandataire HTTP ou de l'accès au serveur Smart Software Manager sur site à partir du périphérique.

- Configurez un serveur DNS pour que le périphérique puisse résoudre le nom du Smart Software Manager.
- Réglez l'horloge du périphérique. Sur le Firepower 2100 en mode plateforme, vous réglez l'horloge dans FXOS.
- Créez un compte sur le Cisco Smart Software Manager :

  https://software.cisco.com/#module/SmartLicensing

  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte pour votre organisation.

Conditions préalables à la réservation de licence permanente

- Créez un compte principal sur le Cisco Smart Software Manager :

  https://software.cisco.com/#module/SmartLicensing

  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation. Même si l'ASA a besoin d'une connectivité Internet au serveur de licences Smart pour la réservation de licence permanente, Smart Software Manager est utilisé pour gérer vos licences permanentes.
- Obtenez une assistance pour la réservation de licence permanente de l'équipe chargée des licences. Vous devez fournir une justification pour utiliser la réservation de licence permanente. Si votre compte n'est pas approuvé, vous ne pouvez pas acheter et appliquer de licences permanentes.
- Achetez des licences permanentes spéciales. Si vous n'avez pas la bonne licence dans votre compte, lorsque vous essayez de réserver une licence sur l'ASA, vous verrez un message d'erreur ressemblant à : « Les licences ne peuvent pas être réservées, car le compte virtuel ne contient pas un surplus suffisant des licences permanentes suivantes : 1 – Firepower 4100 ASA PERM UNIV (perpétuelle) ».
- La licence permanente comprend toutes les fonctionnalités disponibles, y compris la licence de cryptage renforcé (3DES/AES), si votre compte est admissible. Les fonctionnalités Secure Client (services client sécurisés) sont également activées au maximum de la plateforme, selon votre achat d'une licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 133).
- ASA virtuel : la réservation de licence permanente n'est pas prise en charge pour l'hyperviseur Azure.

Gestion des licences logicielles Smart

- Seules les licences logicielles Smart sont prises en charge. Pour les anciens logiciels sur l'ASA virtuel, si vous mettez à niveau un ASA virtuel sous licence PAK existant, la clé d'activation précédemment installée sera ignorée, mais conservée sur l'appareil. Si vous rétrogradez l'ASA virtuel, la clé d'activation sera rétablie.
- Pour la réservation de licence permanente, vous devez retourner la licence avant de désactiver l'appareil. Si vous ne retournez pas officiellement la licence, la licence reste dans un état usagé et ne peut pas être réutilisée pour un nouvel appareil.

- Étant donné que la passerelle de transmission Cisco utilise un certificat avec un code de pays non conforme, vous ne pouvez pas utiliser HTTPS lorsque vous utilisez l'ASA en conjonction avec ce produit. Vous devez utiliser HTTP avec la passerelle de transmission Cisco.

Paramètres par défaut des licences logicielles Smart

Profil Smart Call Home

La configuration par défaut pour tous les modèles, à l'exception des modèles Firepower 4100/9300 (qui active la communication de la licence logicielle Smart au niveau du châssis), comprend un profil Smart Call Home appelé « Licence » qui spécifie l'URL de Smart Software Manager.

ASA virtuel

- Lorsque vous déployez l'ASA virtuel, vous définissez le niveau de fonctionnalité et le niveau de débit. Seul le niveau Essentials est disponible pour le moment. Pour la réservation de licence permanente, vous n'avez pas besoin de définir ces paramètres. Lorsque vous activez la réservation de licence permanente, ces commandes sont supprimées de la configuration.

Remarque La licence Essentials était connue sous le nom de licence Standard, et l'interface de ligne de commande utilise toujours la terminologie « Standard ».

ASA virtuel : configurer les licences logicielles Smart

Cette section décrit comment configurer les licences logicielles Smart pour ASA virtuel.

ASA virtuel : configurer les licences logicielles Smart standard

Lorsque vous déployez l'ASA virtuel, vous pouvez préconfigurer le périphérique et inclure un jeton d'enregistrement afin qu'il s'enregistre auprès du Smart Software Manager et active les licences logicielles Smart. Si vous devez modifier votre serveur mandataire HTTP, vos droits de licence ou enregistrer l'ASA virtuel (par exemple, si vous n'avez pas inclus le jeton d'identification dans la configuration Day0), effectuez cette tâche.

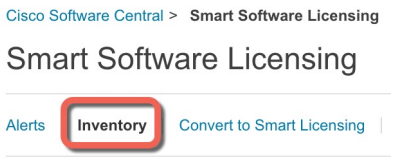
Remarque Vous avez peut-être préconfiguré le mandataire HTTP et les droits de licence lorsque vous avez déployé votre ASA virtuel. Vous avez peut-être également inclus le jeton d'enregistrement dans votre configuration Day0 lorsque vous avez déployé l'ASA virtuel; si tel est le cas, vous n'avez pas besoin de vous réinscrire en utilisant cette procédure.

Procédure

Étape 1 (Cisco Smart Software Manager), demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce périphérique.

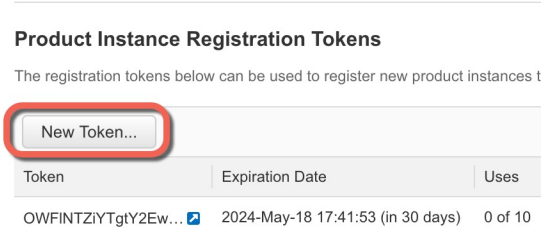
a) Cliquez sur **Inventory** (Inventaire).

Illustration 16 : Inventaire



b) Dans l'onglet **General** (Général), cliquez sur **New Token** (Nouveau jeton).

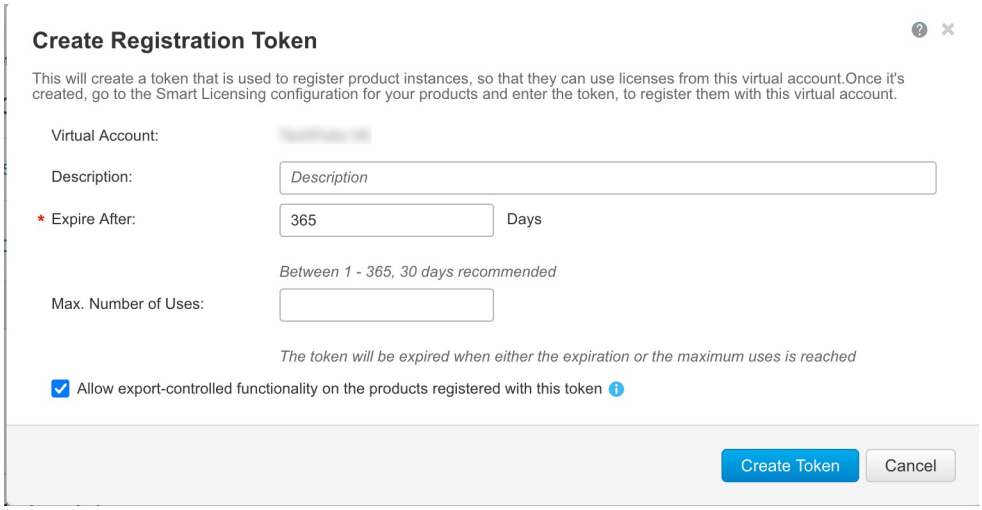
Illustration 17 : Nouveau jeton



c) Dans la boîte de dialogue **Create Registration Token** (Créer un jeton d'enregistrement), entrez les paramètres suivants, puis cliquez sur **Create Token** (Créer un jeton) :

- **Description**
- **Expire After** (Expiration après) : Cisco recommande 30 jours.
- **Nombre max. d'utilisations**
- **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton) : active l'indicateur de conformité à l'exportation.

Illustration 18 : Créer un jeton d'enregistrement



Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône de flèche à droite du jeton pour ouvrir la boîte de dialogue **Token** (Jeton) afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Gardez ce jeton prêt pour plus tard dans la procédure lorsque vous devez enregistrer ASA.

Illustration 19 : Afficher le jeton

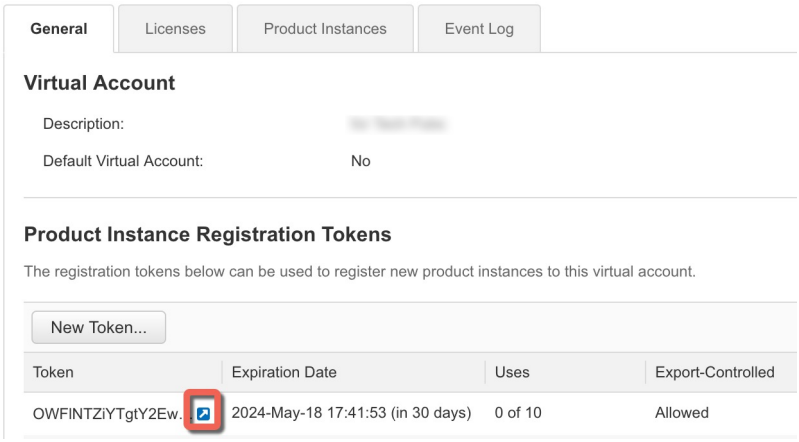
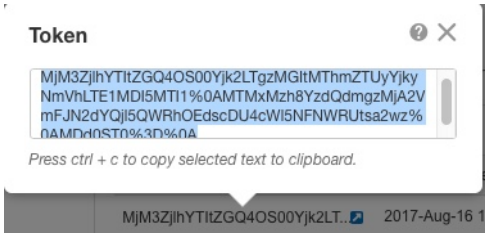


Illustration 20 : Copier le jeton



Étape 2 (Facultatif) Sur l'ASA, spécifiez l'URL du mandataire HTTP pour Call Home :

Si votre réseau utilise un mandataire HTTP pour l'accès Internet, vous devez configuer l'adresse du mandataire pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Call Home en général.



Remarque Le mandataire HTTP avec l'authentification n'est pas pris en charge.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.
b) Cochez **Enable HTTP Proxy** (Activer le serveur mandataire HTTP).
c) Saisissez l'adresse IP et le port du mandataire dans les champs **Proxy server** (Serveur du mandataire) et **Proxy port** (Port du mandataire). Par exemple, saisissez le port 443 pour un serveur HTTPS.
d) Cliquez sur **Apply** (Appliquer).

Étape 3 Configurez les droits de licence :

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cochez la case **Enable Smart license configuration** (Activer la configuration de licence Smart).
c) Dans la liste déroulante **Feature Tier** (Niveau de fonctionnalité), choisissez **Essentials**.

Seul le niveau Essentials est disponible, cependant, vous devez l'activer dans la configuration.

d) Dans la liste déroulante **Throughput Level** (Niveau de débit), choisissez l'une des options suivantes : **100M**, **1G**, **2G**, **10G**, **20G**.

Consultez la relation débit/licence suivante :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

e) (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé). **Ne cochez pas** cette case si vous recevez le jeton de cryptage renforcé.

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

f) Cliquez sur **Apply** (Appliquer).

Étape 4 Enregistrez l'ASA virtuel auprès du Smart Software Manager

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cliquez sur **Register** (Inscrire).
c) Saisissez le jeton d'enregistrement dans le champ **ID Token** (Jeton d'ID).
d) (Facultatif) Cliquez sur la case **Force registration** (Forcer l'enregistrement) pour enregistrer l'ASA virtuel déjà enregistré s'il n'est pas synchronisé avec Smart Software Manager.

Par exemple, utilisez **Force registration** (Forcer l'enregistrement) si l'ASA virtuel a été accidentellement retiré de Cisco Smart Software Manager.

e) Cliquez sur **Register** (Inscrire).

L'ASA virtuel tente de s'enregistrer auprès de Smart Software Manager et demande l'autorisation pour les droits de licence configurés.

Lorsque vous enregistrez l'ASA virtuel, Smart Software Manager émet un certificat d'ID pour la communication entre l'ASA virtuel et Smart Software Manager. Il affecte également l'ASA virtuel au compte virtuel approprié. Normalement, cette procédure est une instance unique. Cependant, vous devrez peut-être réenregistrer ultérieurement l'ASA virtuel. Par exemple, le certificat d'identification expire en raison d'un problème de communication.

ASA virtuel : configurer les licences Smart Software Manager sur site

Cette procédure s'applique pour l'ASA virtuel à l'aide de Smart Software Manager sur site.

Avant de commencer

- Téléchargez le fichier OVA Smart Software Manager sur site à partir de Cisco.com, installez-le et configurez-le sur un serveur VMwareESXi. Pour en savoir plus, consultez la *fiche technique de Cisco Smart Software Manager sur site*.
- Téléchargez le groupe de confiance CA de chiffrement avant de placer l'appareil dans un réseau isolé. Ce groupe de confiance est normalement téléchargé automatiquement, mais peut être obsolète dans un réseau isolé :

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

Procédure

Étape 1 Demandez un jeton d'enregistrement sur Smart Software Manager sur site.

Étape 2 (Facultatif) Sur l'ASA virtuel, spécifiez l'URL du mandataire HTTP pour Call Home :

Remarque Le mandataire HTTP avec l'authentification n'est pas pris en charge.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.
b) Cochez **Enable HTTP Proxy** (Activer le serveur mandataire HTTP).
c) Saisissez l'adresse IP et le port du mandataire dans les champs **Proxy server** (Serveur du mandataire) et **Proxy port** (Port du mandataire). Par exemple, saisissez le port 443 pour un serveur HTTPS.
d) Cliquez sur **Apply** (Appliquer).

Étape 3 Changez l'URL du serveur de licence pour accéder à Smart Software Manager sur site.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.

b) Dans la zone **Configure Subscription Profiles** (Configurer les profils d'abonnement), modifiez le profil **License** (Licence).
c) Dans la zone **Deliver Subscriptions Using HTTP transport** (Fournir les abonnements à l'aide du transport HTTP), sélectionnez l'URL **Subscribers** (Abonnés), puis cliquez sur **Edit** (Modifier).
d) Modifiez l'URL **Subscribers** (Abonnés) à la valeur suivante, puis cliquez sur **OK** :

https://*on-prem_ip_address***/Transportgateway/services/DeviceRequestHandler**

e) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Étape 4 Sur l'ASA virtuel, configurez les droits de licence.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cochez la case **Enable Smart license configuration** (Activer la configuration de licence Smart).
c) Dans le menu déroulant **Feature Tier** (Niveau de fonctionnalités), choisissez **Essentials**.

Seul le niveau **Essentials** est disponible, cependant, vous devez l'activer dans la configuration.

d) Pour déterminer la licence demandée au Smart Software Manager, dans la liste déroulante **Throughput Level** (Niveau de débit), choisissez l'une des options suivantes : **100M**, **1G**, **2G**, **10G**, **20G**.

Consultez la relation débit/licence suivante :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

e) (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé). **Ne cochez pas** cette case si vous recevez le jeton de cryptage renforcé.

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

f) Cliquez sur **Apply** (Appliquer).

Étape 5 Enregistrez l'ASA auprès du Smart Software Manager.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cliquez sur **Register** (Inscrire).
c) Saisissez le jeton d'enregistrement dans le champ **ID Token** (Jeton d'ID).
d) (Facultatif) Cochez la case **Force registration** (Forcer l'enregistrement) pour enregistrer un ASA déjà enregistré s'il n'est pas synchronisé avec Smart Software Manager.

Par exemple, utilisez **Force registration** (Forcer l'enregistrement) si l'ASA a été accidentellement retiré de Smart Software Manager.

e) Cliquez sur **Register** (Inscrire).

L'ASA s'enregistre auprès de Smart Software Manager et demande l'autorisation pour les droits de licence configurés. Le Cisco Smart Software Manager applique également la licence de cryptage renforcé (3DES/AES) si votre compte le permet. Choisissez **Monitoring (Supervision) > Properties (Propriétés) > Smart License (Licence Smart)** pour vérifier l'état de la licence.

Lorsque vous enregistrez l'ASA virtuel, Smart Software Manager émet un certificat d'ID pour la communication entre l'ASA virtuel et Smart Software Manager. Il affecte également l'ASA virtuel au compte virtuel approprié. Normalement, cette procédure est une instance unique. Cependant, vous devrez peut-être réenregistrer ultérieurement l'ASA virtuel si le certificat d'ID expire en raison d'un problème de communication, par exemple.

ASA virtuel: configurer les licences logicielles Smart Utility (MSLA)

La licence utilitaire pour un contrat de licence de services gérés (MSLA) vous permet de payer la durée d'utilisation d'une licence plutôt que de payer des frais ponctuels pour un abonnement à une licence ou une licence permanente. En mode de licence utilitaire, l'ASA virtuel suit l'utilisation des licences en unités de temps (intervalles de 15 minutes). L'ASA virtuel envoie des rapports d'utilisation des licences (aussi appelés rapports sur la mesure de l'utilisation des ressources) à Smart Software Manager toutes les quatre heures. Les rapports d'utilisation sont ensuite acheminés à un serveur de facturation. Avec les licences utilitaires, Smart Call Home n'est pas utilisé comme transport pour les messages de licence. Au lieu de cela, les messages sont envoyés directement via HTTP/HTTPS à l'aide de *Smart Transport.*

Avant de commencer

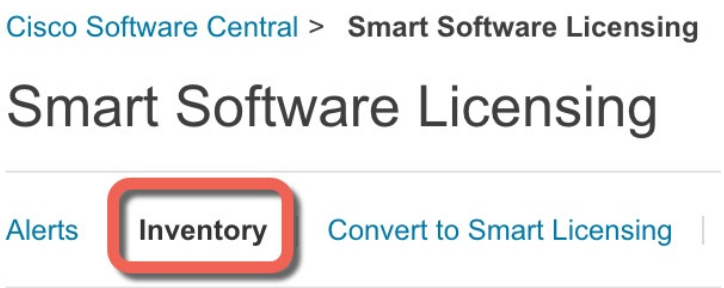
Téléchargez le fichier OVA Smart Software Manager sur site à partir de Cisco.com, installez-le et configurez-le sur un serveur VMware ESXi. Pour en savoir plus, consultez la *fiche technique de Cisco Smart Software Manager sur site*.

Procédure

Étape 1 Dans Smart Software Manager On-Prem, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce périphérique.

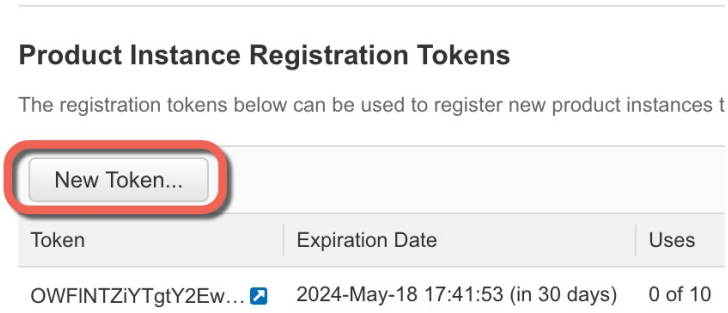
a) Cliquez sur **Inventory** (Inventaire).

Illustration 21 : Inventaire



b) Dans l'onglet **General** (Général), cliquez sur **New Token** (Nouveau jeton).

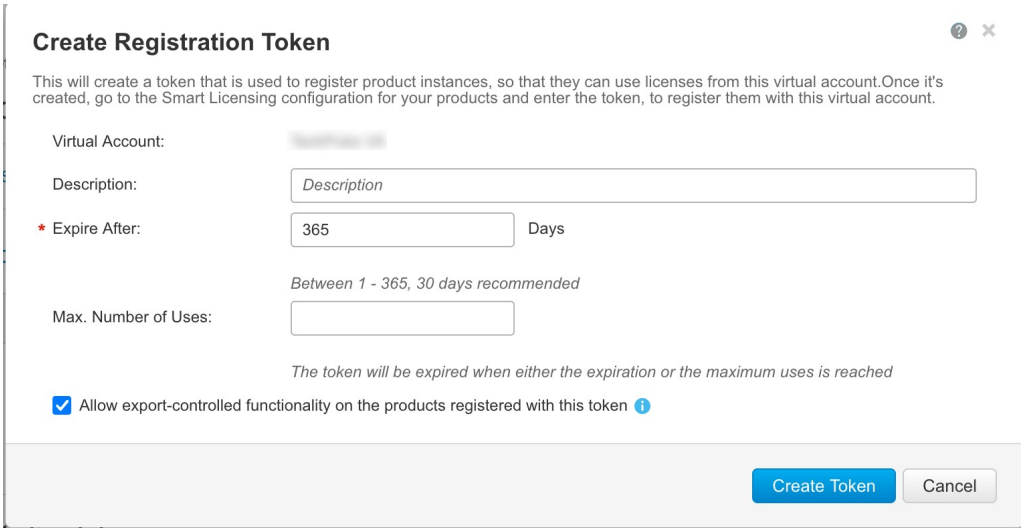
Illustration 22 : Nouveau jeton



c) Dans la boîte de dialogue **Create Registration Token** (Créer un jeton d'enregistrement), entrez les paramètres suivants, puis cliquez sur **Create Token** (Créer un jeton) :

- **Description**
- **Expire After** (Expiration après) : Cisco recommande 30 jours.
- **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton) : active l'indicateur de conformité à l'exportation.

Illustration 23 : Créer un jeton d'enregistrement



Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône de flèche à droite du jeton pour ouvrir la boîte de dialogue **Token** (Jeton) afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Gardez ce jeton prêt pour plus tard dans la procédure lorsque vous devez enregistrer ASA.

Illustration 24 : Afficher le jeton

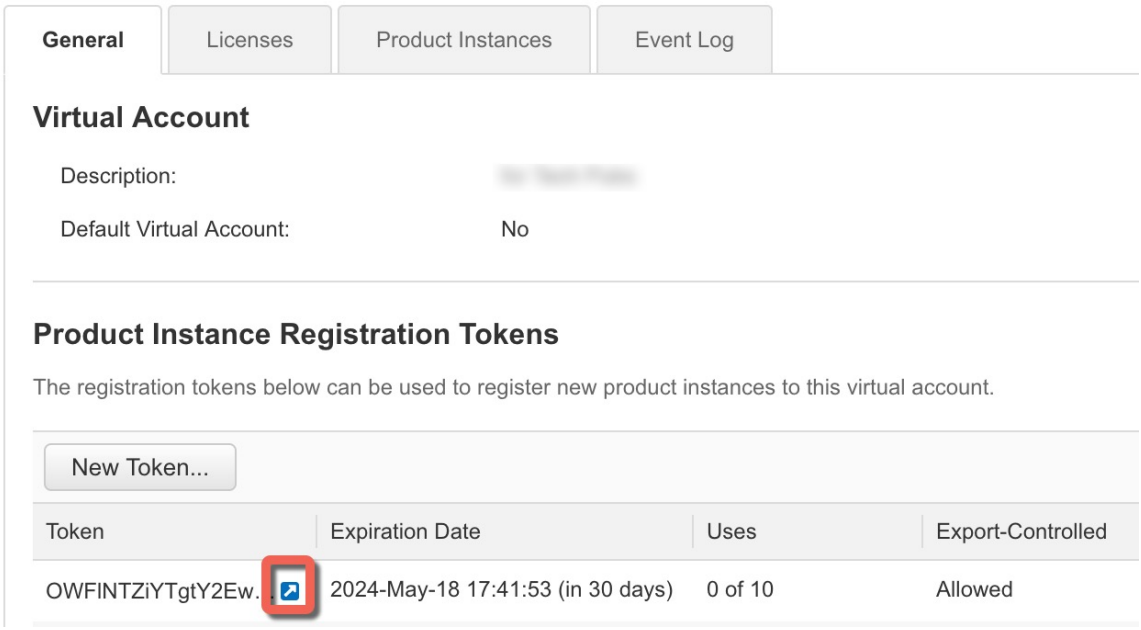
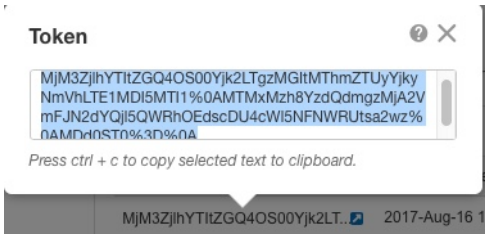


Illustration 25 : Copier le jeton



Étape 2 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 3 Configurez les droits de licence :

a) Cochez la case **Enable Smart license configuration** (Activer la configuration de licence Smart).

b) Dans le menu déroulant **Feature Tier** (Niveau de fonctionnalités), choisissez **Essentials**.

Seul le niveau **Essentials** est disponible, cependant, vous devez l'activer dans la configuration.

c) Pour déterminer la licence demandée au Smart Software Manager, dans la liste déroulante **Throughput Level** (Niveau de débit), choisissez l'une des options suivantes : **100M**, **1G**, **2G**, **10G**, **20G**.

Consultez la relation de débit et de licence suivante :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

d) (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé).

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Étape 4 (Facultatif) Si vous souhaitez supprimer le nom d'hôte ou le numéro de version Smart Agent du périphérique de licence dans les messages de licence, cochez les cases suivantes :

a) **Nom de l'hôte**.
b) **Version**.

Étape 5 Cliquez sur le bouton radio **Smart Transport**.

Étape 6 Configurez les URL pour Smart Transport.

a) Cliquez sur le bouton radio **Custom URL** (URL personnalisée) et saisissez l'URL dans le champ **URL**.
b) Dans le champ **Registration** (Enregistrement), collez le jeton d'enregistrement Smart Software Manager standard ou sur site.
c) Dans le champ **Utility** (Utilitaire), spécifiez l'URL de Smart Software Manager standard ou sur site.
d) (Facultatif) Dans le champ **Proxy URL** (URL du mandataire), spécifiez l'URL du mandataire si le serveur de licences ou le satellite n'est accessible que par un mandataire.

Remarque Le mandataire HTTP avec l'authentification n'est pas pris en charge.

e) (Facultatif) Dans le champ **Proxy Port** (Port du mandataire), spécifiez le numéro de port du mandataire.

Étape 7 Cochez la case **Enable Standard Utility Mode** (Activer le mode utilitaire standard).

Étape 8 Configurez les renseignements de licence de l'utilitaire, qui comprennent les renseignements du client nécessaires à la facturation.

a) Dans le champ **Custom ID** (ID personnalisé), indiquez un identifiant client unique. Cet identifiant est inclus dans les messages du rapport d'utilisation des licences utilitaires.
b) Remplissez le profil du client en saisissant les renseignements appropriés dans les champs restants, notamment **Customer Company Identifier** (Identifiant de l'entreprise du client), **Customer Company Name** (Nom de l'entreprise du client), **Customer Street (Adresse du client)**, **Customer City** (Ville du client), **Customer State** (État du client), **Customer Country** (Pays du client) et **Customer Postal Code** (Code postal du client).

Étape 9 Cliquez sur **Apply** (Appliquer).

Étape 10 Cliquez sur **Register** (Enregistrer) pour enregistrer l'ASA virtuel avec le Smart Software Manager standard ou sur site.

L'ASA s'enregistre auprès de Smart Software Manager et demande l'autorisation pour les droits de licence configurés. Choisissez **Monitoring (Supervision) > Properties (Propriétés) > Smart License (Licence Smart)** pour vérifier l'état de la licence.

ASA virtuel: configurer la réservation de licence permanente

Vous pouvez attribuer une licence permanente à l'ASA virtuel. Cette section décrit également comment restituer une licence si vous retirez l'ASA virtuel ou si vous modifiez les niveaux de modèle et que vous avez besoin d'une nouvelle licence.

Procédure

Étape 1 Installer la licence permanente ASA virtuel, à la page 159

Étape 2 (Facultatif) Retourner la licence permanente ASA virtuel, à la page 161

Installer la licence permanente ASA virtuel

Pour un ASA virtuel qui n'a pas d'accès Internet, vous pouvez demander une licence permanente auprès de Smart Software Manager. Pour en savoir plus sur la réservation de licence permanente ASA virtuel, consultez Réservation de licence permanente pour l'ASA virtuel, à la page 127.

Remarque

- Pour la réservation de licence permanente, vous devez retourner la licence avant de désactiver l'ASA virtuel. Si vous ne retournez pas officiellement la licence, la licence reste dans un état usagé et ne peut pas être réutilisée pour un nouvel ASA virtuel. Consultez (Facultatif) Retourner la licence permanente ASA virtuel, à la page 161.
- Si vous effacez votre configuration après avoir installé la licence permanente, par exemple, en utilisant la commande **write erase**, vous n'avez qu'à réactiver la réservation de licence permanente à l'aide de la commande **license smart reservation** sans arguments, vous n'avez pas besoin de terminer le reste de cette procédure.

Avant de commencer

- Achetez des licences permanentes pour qu'elles soient disponibles dans Smart Software Manager. Tous les comptes ne sont pas approuvés pour la réservation de licence permanente. Assurez-vous d'avoir l'approbation de Cisco pour cette fonctionnalité avant de tenter de la configurer.
- Demandez une licence permanente après le démarrage d'ASA virtuel; vous ne pouvez pas installer de licence permanente dans le cadre de la configuration du jour 0.

Procédure

Étape 1 (ASAv5 uniquement) Exécutez cette commande pour autoriser l'utilisation de la licence permanente ASAv5 lorsque la DRAM est de 2 Go (le minimum requis dans la version 9.13 et les versions ultérieures) :

license smart set_plr5

Étape 2 Activez la réservation de licence permanente à partir de l'interface de ligne de commande de l'ASA virtuel :

license smart reservation

Exemple :

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

Pour utiliser une licence Smart standard, utilisez la forme **no** de cette commande .

Les commandes suivantes sont supprimées :

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G}
```

Étape 3 Demandez le code de licence à saisir dans Smart Software Manager :

license smart reservation request universal

Exemple :

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

si vous modifiez la mémoire ou les vCPU, vous devrez renvoyer la licence actuelle et demander une nouvelle licence au nouveau niveau de modèle. La licence demandée doit correspondre à la mémoire et aux vCPU installées. Pour en savoir plus sur la vCPU et la matrice de mémoire en licence pour la réservation de licence permanente d'ASA virtuel, consultez Réservation de licence permanente pour l'ASA virtuel, à la page 127.

Pour modifier le modèle d'un ASA virtuel déjà déployé, à partir de l'hyperviseur, vous pouvez modifier les paramètres des vCPU et de la DRAM pour qu'ils correspondent aux exigences du nouveau modèle; consultez le guide de démarrage rapide d'ASA virtuel pour connaître ces valeurs. Pour afficher votre modèle actuel, utilisez la commande **show vm**.

Si vous saisissez à nouveau cette commande, le même code s'affiche, même après un rechargement. Si vous n'avez pas encore saisi ce code dans Smart Software Manager et que vous souhaitez annuler la demande, saisissez :

license smart reservation cancel

Si vous désactivez la réservation de licence permanente, toutes les demandes en attente sont annulées. Si vous avez déjà saisi le code dans Smart Software Manager, vous devez effectuer cette procédure pour appliquer la licence à l'ASA virtuel, après quoi vous pouvez renvoyer la licence si vous le souhaitez. Consultez (Facultatif) Retourner la licence permanente ASA virtuel, à la page 161.

Étape 4 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Licenses** (Licences) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Licenses** (Licences) affiche toutes les licences existantes liées à votre compte, standard et permanentes.

Étape 5 Cliquez sur **License Reservation** (Réservation de licence) et saisissez le code de l'ASA virtuel dans le champ **Reservation Request Code** (Code de demande de réservation).

Étape 6 Cliquez sur **Reserve License** (Réserver la licence).

Smart Software Manager génère un code d'autorisation. Vous pouvez télécharger le code ou le copier dans le presse-papiers. À ce stade, la licence est utilisée selon Smart Software Manager.

Si vous ne voyez pas de bouton **License Reservation** (Réservation de licence), votre compte n'est pas autorisé pour la réservation de licence permanente. Dans ce cas, vous devez désactiver la réservation de licence permanente et saisir les commandes de licence Smart normales.

Étape 7 À partir de l'interface de ligne de commande de l'ASA virtuel, exécutez la commande suivante et saisissez le code d'autorisation :

license smart reservation install *code*

Exemple :

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
INFO: ASAv platform license state is Licensed.
ciscoasa#
```

Votre ASA virtuel a maintenant une licence complète.

Étape 8 Exécutez cette commande pour enregistrer la configuration en cours d'exécution dans la configuration de démarrage afin d'éviter toute perte de configuration lors du redémarrage.

write memory

Étape 9 À partir de l'ASA virtuel, exécutez cette commande pour afficher et confirmer que l'ASA dispose de la licence permanente.

show license features

(Facultatif) Retourner la licence permanente ASA virtuel

Si vous n'avez plus besoin d'une licence permanente, par exemple, vous retirez l'ASA virtuel ou modifiez son niveau de modèle, en raison duquel il a besoin d'une nouvelle licence, vous devez officiellement retourner la licence à Smart Software Manager en utilisant cette procédure. Si vous ne suivez pas toutes les étapes, la licence reste dans un état utilisé et ne peut pas être libérée pour être utilisée ailleurs.

Procédure

Étape 1 À partir de l'interface de ligne de commande d'ASA virtuel, générez un code de retour :

license smart reservation return

Exemple :

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

L'ASA virtuel devient immédiatement sans licence et passe à l'état d'évaluation. Si vous devez afficher de nouveau ce code, ressaisissez cette commande. Notez que si vous demandez une nouvelle licence permanente (**license smart reservation request universal**) ou si vous modifiez le niveau de modèle d'ASA virtuel (en

activant et en modifiant les vCPU/RAM), vous ne pouvez pas réafficher ce code. Assurez-vous de capturer le code pour terminer le retour.

Étape 2 Affichez l'identifiant universel d'appareil (UDI) ASA virtuel pour vous permettre de trouver votre instance ASA virtuel dans Smart Software Manager.

show license udi

Exemple :

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

Étape 3 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Product Instances** (Instances de produit) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Product Instances** (Instances de produit) affiche tous les produits sous licence par l'UDI.

Étape 4 Recherchez l'ASA virtuel dont vous souhaitez annuler la licence, choisissez **Actions** > **Remove (Supprimer)** et saisissez le code de retour ASA virtuel dans le champ **Reservation Return Code** (Code de retour de réservation).

La licence permanente est renvoyée vers l'ensemble disponible.

Étape 5 Cliquez sur **Remove Product Instance** (Supprimer l'instance de produit) (Supprimer la réservation).

Étape 6 Pour désactiver la réservation de licence permanente, procédez comme suit :

a) Exécutez la commande suivante pour désactiver la réservation de licence permanente :

no license smart reservation

b) Exécutez la commande suivante pour confirmer que la licence est annulée :

show license features

La sortie de la commande affiche `No active allowed` (Aucun droit actif).

Étape 7 Exécutez cette commande pour enregistrer la configuration en cours d'exécution dans la configuration de démarrage afin d'éviter toute perte de configuration lors du redémarrage.

write memory

(Facultatif) Annuler l'enregistrement de l'ASA virtuel (standard et sur site)

L'annulation de l'enregistrement de l'ASA virtuel supprime l'ASA virtuel de votre compte. Tous les droits de licence et tous les certificats de l'ASA virtuel sont supprimés. Vous souhaiterez peut-être vous désinscrire pour libérer une licence pour un nouvel ASA virtuel. Sinon, vous pouvez supprimer l'ASA virtuel du Smart Software Manager.

Remarque Si vous annulez l'enregistrement de l'ASA virtuel, il reviendra à un état de débit fortement limité après avoir rechargé l'ASA virtuel.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 2 Cliquez sur **Unregister** (Annuler l'enregistrement).

L'ASA virtuel se recharge ensuite.

(Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASA virtuel (standard et sur site)

Par défaut, le certificat d'ID est automatiquement renouvelé tous les six mois et le droit de licence est renouvelé tous les 30 jours. Vous pourriez souhaiter renouveler manuellement l'enregistrement de l'un de ces éléments si vous avez une fenêtre limitée pour l'accès Internet, ou si vous apportez des modifications de licence dans Smart Software Manager, par exemple.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 2 Pour renouveler le certificat d'ID, cliquez sur **Renew ID Certificate** (Renouveler le certificat d'ID).

Étape 3 Pour renouveler le droit de licence, cliquez sur **Renew Authorization** (Renouveler l'autorisation).

Firepower 4100/9300 : configuration de la licence logicielle Smart

Cette procédure s'applique pour un châssis utilisant Smart Software Manager, Smart Software Manager sur site ou pour la réservation de licence permanente; consultez le guide de configuration FXOS pour pré-configurer la communication de licences.

Pour la réservation de licence permanente, la licence active toutes les fonctionnalités : le niveau standard avec le nombre maximum de contextes de sécurité et la licence de l'opérateur. Cependant, pour que l'ASA « sache » utiliser ces fonctionnalités, vous devez les activer sur l'ASA.

Avant de commencer

Pour une grappe ASA, vous devez accéder au nœud de contrôle pour la configuration. Vérifiez le Firewall Chassis Manager pour voir quel nœud est le nœud de contrôle.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 2 Dans la liste déroulante **Feature Tier** (niveaux de fonctionnalités), choisissez **Standard**.

Seul le niveau standard est disponible. Une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités. Vous devez avoir suffisamment de licences de niveau dans votre compte. Sinon, vous ne pouvez pas configurer d'autres licences de fonctionnalités ou des fonctionnalités nécessitant des licences.

Étape 3 (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé). **Ne cochez pas** cette case si vous recevez le jeton de cryptage renforcé.

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Étape 4 (Facultatif) Cochez la case (Fournisseur de services mobiles)**Carrier** (Opérateur).

Étape 5 (Facultatif) Dans la liste déroulante **Context** (Contexte), choisissez le nombre de contextes souhaités.

Pour la réservation de licence permanente, vous pouvez spécifier le nombre de contextes maximum (248).

Étape 6 Cliquez sur **Apply** (Appliquer).

Étape 7 Quittez ASDM, puis relancez-le.

Lorsque vous modifiez les licences, vous devez relancer ASDM pour afficher les écrans mis à jour.

Autres modèles : configurer les licences logicielles Smart

Cette section décrit comment configurer les licences logicielles Smart pour les modèles suivants

- Firepower 1010
- Firepower 1100
- Firepower 2100
- Secure Firewall 3100

À cette fin, choisissez l'une des méthodes suivantes :

• Autres modèles : configurer les licences logicielles Smart standard, à la page 165

Vous pouvez également (Autres modèles) Dérégistrer l'ASA (standard et sur site), à la page 177 ou (Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASAv (standard et sur site), à la page 178.

- Autres modèles : configuration des licences Smart Software Manager sur site, à la page 170

  Vous pouvez également (Autres modèles) Dérégistrer l'ASA (standard et sur site), à la page 177 ou (Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASAv (standard et sur site), à la page 178.

- Autres modèles : configuration de la réservation de licence permanente, à la page 173

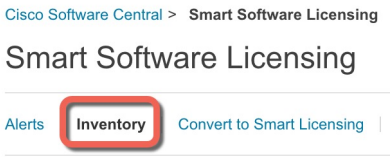
Autres modèles : configurer les licences logicielles Smart standard

Cette procédure s'applique à un ASA utilisant Smart Software Manager.

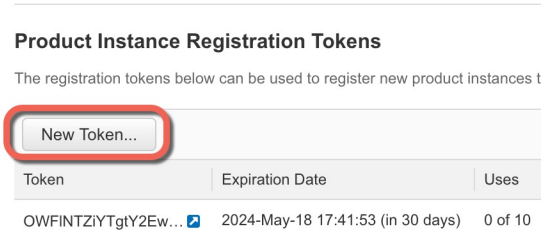
Procédure

Étape 1 Dans Cisco Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce périphérique.

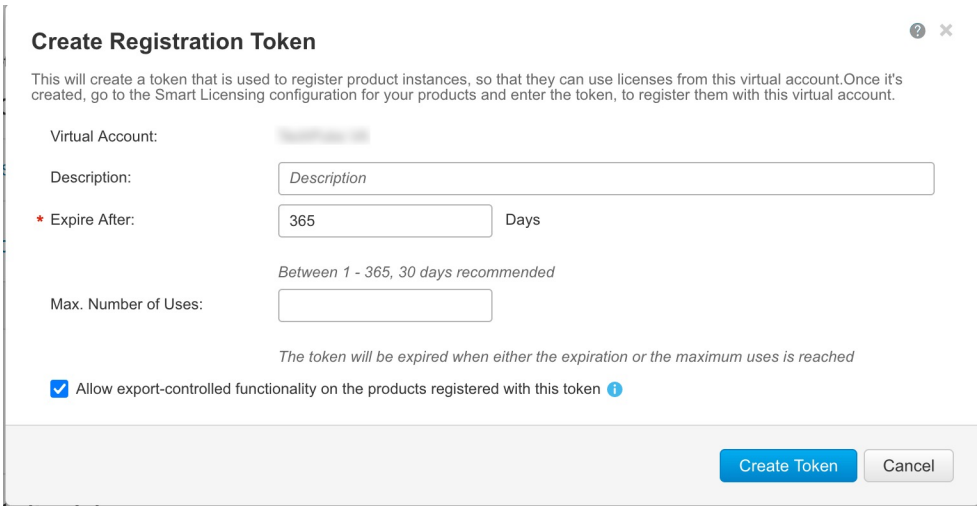
a) Cliquez sur **Inventory** (Inventaire).



b) Dans l'onglet **General** (Général), cliquez sur **New Token** (Nouveau jeton).



c) Dans la boîte de dialogue **Create Registration Token** (Créer un jeton d'enregistrement), entrez les paramètres suivants, puis cliquez sur **Create Token** (Créer un jeton) :



- **Description**
- **Expire After** (Expiration après) : Cisco recommande 30 jours.
- **Nombre max. d'utilisations**
- **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton) : active l'indicateur de conformité à l'exportation.

Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône de flèche à droite du jeton pour ouvrir la boîte de dialogue **Token** (Jeton) afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Conservez ce jeton à portée de main pour la suite de la procédure, lorsque vous devrez enregistrer l'ASA.

Illustration 26 : Afficher le jeton

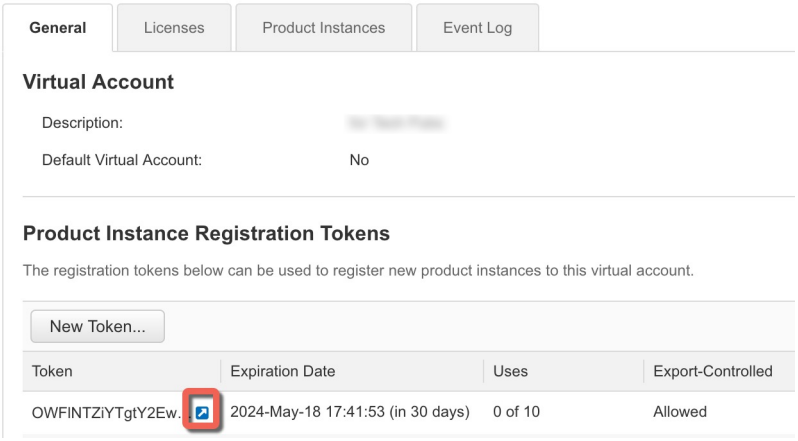
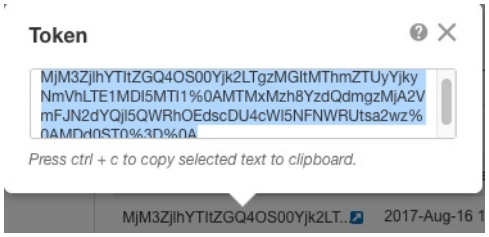


Illustration 27 : Copier le jeton



Étape 2 (Facultatif) Sur l'ASA, spécifiez l'URL du mandataire HTTP pour Call Home :

Si votre réseau utilise un mandataire HTTP pour l'accès Internet, vous devez configuer l'adresse du mandataire pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Call Home en général.

Remarque Le mandataire HTTP avec l'authentification n'est pas pris en charge.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.
b) Cochez la case **Enable HTTP Proxy** (Activer le mandataire HTTP).
c) Saisissez l'adresse IP et le port du mandataire dans les champs **Proxy Server** (Serveur du mandataire) et **Proxy Port** (Port du mandataire). Par exemple, saisissez le port 443 pour un serveur HTTPS.
d) Cliquez sur **Apply** (Appliquer).

Étape 3 Configurez les droits de licence :

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cochez la case **Enable Smart license configuration** (Activer la configuration de licence Smart).
c) Dans le menu déroulant **Feature Tier** (Niveau de fonctionnalités), choisissez **Essentials**.

Seul le niveau **Essentials** est disponible, cependant, vous devez l'activer dans la configuration; une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités. Pour les modèles Secure Firewall, la licence Essentials est toujours activée et ne peut pas être désactivée.

d) (Facultatif) (Firepower 1010) Cochez la case **Enable Security Plus** (Activer Security Plus).

Le niveau Security Plus permet le basculement.

e) (Facultatif) (Modèles pris en charge) Pour la licence **Context** (Contexte), entrez le nombre de contextes.

Par défaut, l'ASA prend en charge 2 contextes. Vous devez donc demander le nombre de contextes souhaités moins les 2 contextes par défaut. Le nombre maximal de contextes dépend de votre modèle :

- Firepower 1120 : 5 contextes
- Firepower 1140 : 10 contextes
- Firepower 1150 : 25 contextes
- Firepower 2110 : 25 contextes
- Firepower 2120 : 25 contextes
- Firepower 2130 : 30 contextes

- Firepower 2140 : 40 contextes
- Cisco Secure Firewall 3100 : 100 contextes

Par exemple, pour utiliser le maximum de 25 contextes de Firepower 1150, saisissez 23 comme nombre de contextes. Cette valeur est ajoutée à la valeur par défaut de 2.

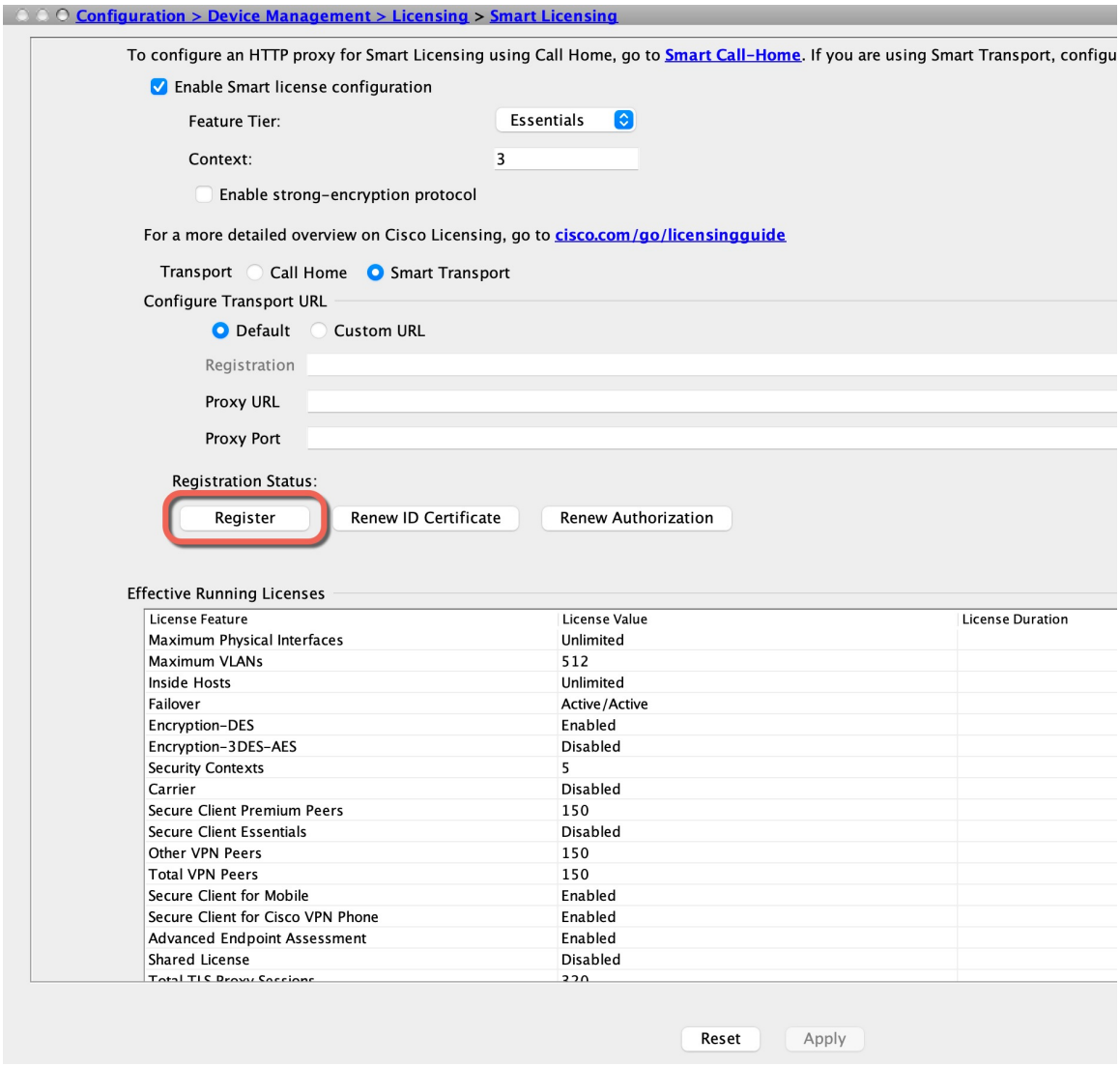
f) (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé). **Ne cochez pas** cette case si vous recevez le jeton de cryptage renforcé.

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

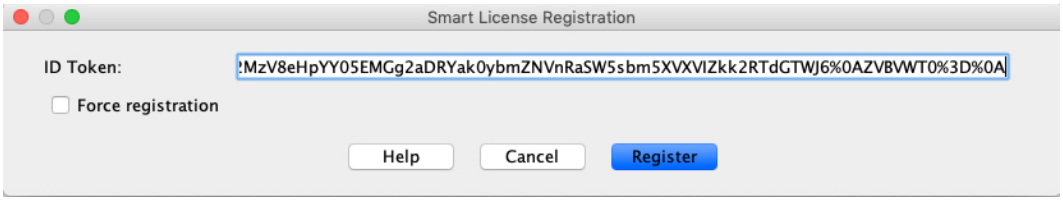
g) (Facultatif) (Modèles pris en charge) Cochez **Enable Carrier** (Activer Carrier) pour l'inspection Diameter, GTP/GPRS et SCTP.

h) Cliquez sur **Apply** (Appliquer).

Étape 4 Cliquez sur **Register** (Enregistrer).



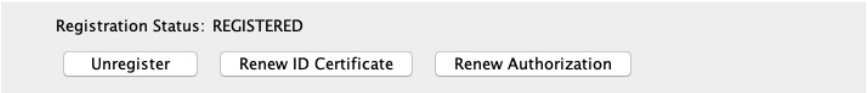
Étape 5 Saisissez le jeton d'enregistrement dans Cisco Smart Software Manager dans le champ **ID Token** (Jeton d'ID).



(Facultatif) Cliquez sur la case **Force registration** (Forcer l'enregistrement) pour enregistrer un ASA déjà enregistré, mais qui pourrait ne pas être synchronisé avec le Smart Software Manager. Par exemple, utilisez **Force registration** si l'ASA a été accidentellement supprimé du Smart Software Manager.

Étape 6 Cliquez sur **Register** (Inscrire).

ASDM actualise la page lorsque l'état de la licence est mis à jour. Vous pouvez également choisir **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Smart License (Licence intelligente)** pour vérifier l'état de la licence, en particulier si l'enregistrement échoue.



Étape 7 Quittez ASDM, puis relancez-le.

Lorsque vous modifiez les licences, vous devez relancer ASDM pour afficher les écrans mis à jour.

Autres modèles : configuration des licences Smart Software Manager sur site

Cette procédure s'applique à un ASA utilisant Smart Software Manager sur site.

Avant de commencer

- Téléchargez le fichier OVA Smart Software Manager sur site à partir de Cisco.com, installez-le et configurez-le sur un serveur VMwareESXi. Pour en savoir plus, consultez la *fiche technique de Cisco Smart Software Manager sur site*.
- Téléchargez le groupe de confiance CA de chiffrement avant de placer l'appareil dans un réseau isolé. Ce groupe de confiance est normalement téléchargé automatiquement, mais peut être obsolète dans un réseau isolé :

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

Procédure

Étape 1 Demandez un jeton d'enregistrement sur le serveur Smart Software Manager sur site.

Étape 2 (Facultatif) Sur l'ASA virtuel, spécifiez l'URL du mandataire HTTP pour Call Home :

Si votre réseau utilise un mandataire HTTP pour l'accès Internet, vous devez configuer l'adresse du mandataire pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Call Home en général.

Remarque Le mandataire HTTP avec l'authentification n'est pas pris en charge.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.
b) Cochez la case **Enable HTTP Proxy** (Activer le mandataire HTTP).
c) Saisissez l'adresse IP et le port du mandataire dans les champs **Proxy server** (Serveur du mandataire) et **Proxy port** (Port du mandataire).

   Par exemple, saisissez le port 443 pour un serveur HTTPS.

d) Cliquez sur **Apply** (Appliquer).

Étape 3 Changez l'URL du serveur de licence pour accéder à Smart Software Manager sur site.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call-Home**.
b) Dans la zone **Configure Subscription Profiles** (Configurer les profils d'abonnement), modifiez le profil **License** (Licence).
c) Dans la zone **Deliver Subscriptions Using HTTP transport** (Fournir les abonnements à l'aide du transport HTTP), sélectionnez l'URL **Subscribers** (Abonnés), puis cliquez sur **Edit** (Modifier).
d) Modifiez l'URL **Subscribers** (Abonnés) à la valeur suivante, puis cliquez sur **OK** :

   https://*on-prem_ip_address*/**Transportgateway/services/DeviceRequestHandler**

e) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Étape 4 Configurez les droits de licence :

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
b) Cochez la case **Enable Smart license configuration** (Activer la configuration de licence Smart).
c) Dans le menu déroulant **Feature Tier** (Niveau de fonctionnalités), choisissez **Essentials**.

   Seul le niveau **Essentials** est disponible, cependant, vous devez l'activer dans la configuration; une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités. Pour les modèles Secure Firewall, la licence Essentials est toujours activée et ne peut pas être désactivée.

d) (Facultatif) (Firepower 1010) Cochez la case **Enable Security Plus** (Activer Security Plus).

   Le niveau Security Plus permet le basculement.

e) (Facultatif) (Modèles pris en charge) Pour la licence **Context** (Contexte), entrez le nombre de contextes.

   Par défaut, l'ASA prend en charge 2 contextes. Vous devez donc demander le nombre de contextes souhaités moins les 2 contextes par défaut. Le nombre maximal de contextes dépend de votre modèle :

   - Firepower 1120 : 5 contextes
   - Firepower 1140 : 10 contextes
   - Firepower 1150 : 25 contextes
   - Firepower 2110 : 25 contextes
   - Firepower 2120 : 25 contextes
   - Firepower 2130 : 30 contextes
   - Firepower 2140 : 40 contextes
   - Cisco Secure Firewall 3100 : 100 contextes

   Par exemple, pour utiliser le maximum de 25 contextes de Firepower 1150, saisissez 23 comme nombre de contextes. Cette valeur est ajoutée à la valeur par défaut de 2.

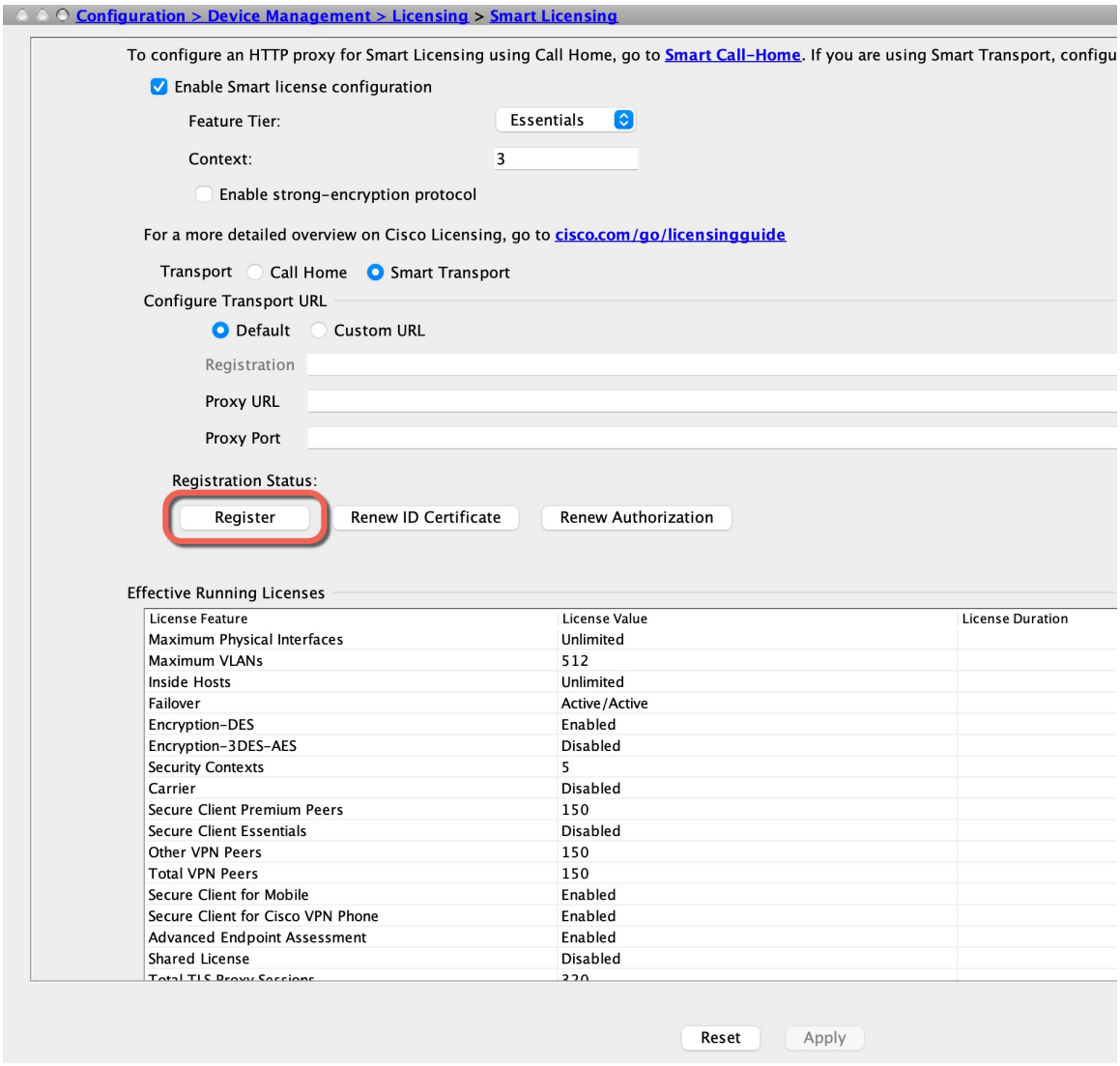
f) (Facultatif) Cochez la case **Enable strong-encryption protocol** (Activer le protocole de cryptage renforcé). **Ne cochez pas** cette case si vous recevez le jeton de cryptage renforcé.

   Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

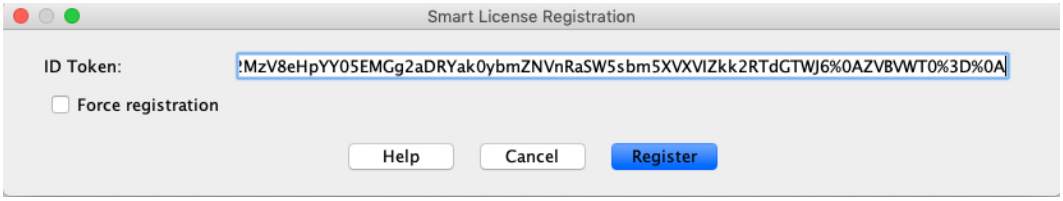
g) (Facultatif) (Modèles pris en charge) Cochez **Enable Carrier** (Activer Carrier) pour l'inspection Diameter, GTP/GPRS et SCTP.

h) Cliquez sur **Apply** (Appliquer).

Étape 5 Cliquez sur **Register** (Enregistrer).



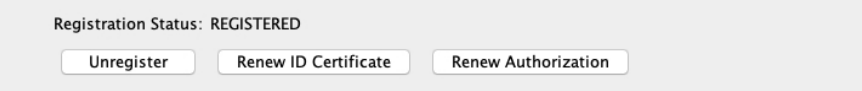
Étape 6 Saisissez le jeton d'enregistrement dans Cisco Smart Software Manager dans le champ **ID Token** (Jeton d'ID).



(Facultatif) Cliquez sur la case **Force registration** (Forcer l'enregistrement) pour enregistrer un ASA déjà enregistré, mais qui pourrait ne pas être synchronisé avec le Smart Software Manager. Par exemple, utilisez **Force registration** si l'ASA a été accidentellement supprimé du Smart Software Manager.

Étape 7 Cliquez sur **Register** (Inscrire).

ASDM actualise la page lorsque l'état de la licence est mis à jour. Vous pouvez également choisir **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Smart License (Licence intelligente)** pour vérifier l'état de la licence, en particulier si l'enregistrement échoue.



Étape 8 Quittez ASDM, puis relancez-le.

Lorsque vous modifiez les licences, vous devez relancer ASDM pour afficher les écrans mis à jour.

Autres modèles : configuration de la réservation de licence permanente

Vous pouvez attribuer une licence permanente. Cette section décrit également comment restituer une licence si vous retirez l'ASA.

Procédure

Étape 1 Installation de la licence permanente 1000/2100/3100, à la page 173.

Étape 2 (Facultatif) Autres modèles : retour de la licence permanente, à la page 176.

Installation de la licence permanente 1000/2100/3100

Pour les ASA qui n'ont pas d'accès Internet, vous pouvez demander une licence permanente auprès de Smart Software Manager. La licence permanente active toutes les fonctionnalités : Essentials licence avec un nombre maximum de contextes de sécurité.

Remarque Pour la réservation de licence permanente, vous devez retourner la licence avant de désactiver l'ASA. Si vous ne retournez pas officiellement la licence, la licence reste dans un état usagé et ne peut pas être réutilisée pour un nouvel ASA. Consultez (Facultatif) Autres modèles : retour de la licence permanente, à la page 176.

Avant de commencer

Achetez des licences permanentes de sorte qu'elles soient disponibles dans Smart Software Manager. Tous les comptes ne sont pas approuvés pour la réservation de licence permanente. Assurez-vous d'avoir l'approbation de Cisco pour cette fonctionnalité avant de tenter de la configurer.

Procédure

Étape 1 Activez la réservation de licence permanente au niveau de l'interface de ligne de commande de l'ASA :

license smart reservation

Exemple :

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

Étape 2 Demandez le code de licence à saisir dans Smart Software Manager :

license smart reservation request universal

Exemple :

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
BB-ZFPR-2140:JAD200802RR-AzKmHcc71-2A
ciscoasa#
```

Si vous saisissez à nouveau cette commande, le même code s'affiche, même après un rechargement. Si vous n'avez pas encore saisi ce code dans Smart Software Manager et que vous souhaitez annuler la demande, saisissez :

license smart reservation cancel

Si vous désactivez la réservation de licence permanente, toutes les demandes en attente sont annulées. Si vous avez déjà saisi le code dans Smart Software Manager, vous devez effectuer cette procédure pour appliquer la licence à l'ASA, après quoi vous pouvez renvoyer la licence si vous le souhaitez. Consultez (Facultatif) Autres modèles : retour de la licence permanente, à la page 176.

Étape 3 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Licenses** (Licences) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Licenses** (Licences) affiche toutes les licences existantes liées à votre compte, standard et permanentes.

Étape 4 Cliquez sur **License Reservation** (Réservation de licence) et saisissez le code ASA dans la zone. Cliquez sur **Reserve License** (Réserver la licence).

Smart Software Manager génère un code d'autorisation. Vous pouvez télécharger le code ou le copier dans le presse-papiers. À ce stade, la licence est utilisée selon Smart Software Manager.

Si vous ne voyez pas de bouton **License Reservation** (Réservation de licence), votre compte n'est pas autorisé pour la réservation de licence permanente. Dans ce cas, vous devez désactiver la réservation de licence permanente et saisir les commandes de licence Smart normales.

Étape 5 Sur l'ASA, saisissez le code d'autorisation :

license smart reservation install *code*

Exemple :

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

Étape 6 Demandez des droits de licence sur l'ASA.



Remarque Bien que la licence permanente permette l'utilisation complète de toutes les licences, vous devez toujours activer les droits dans la configuration ASA pour que l'ASA sache qu'il peut les utiliser.

a) Entrez en mode de configuration de la licence Smart :

license smart

Exemple :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) (Firepower 1000/2100) Définissez le niveau de fonctionnalité :

feature tier standard

Seul le niveau Standard (Essentials) est disponible, cependant, vous devez l'activer dans la configuration; une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités.La licence Essentials était auparavant appelée licence Standard, et « Standard » est toujours utilisé dans l'interface de ligne de commande. Pour les modèles Secure Firewall, la licence Essentials est toujours activée et ne peut pas être désactivée.

c) (Facultatif) (Modèles pris en charge) Demandez la licence de contexte de sécurité.

feature context *number*

Par défaut, l'ASA prend en charge 2 ou contextes, vous devez donc demander le nombre de contextes souhaités moins les contextes par défaut. Le nombre maximal de contextes dépend de votre modèle :

- Firepower 1120 : 5 contextes
- Firepower 1140 : 10 contextes
- Firepower 1150 : 25 contextes
- Firepower 2110 : 25 contextes
- Firepower 2120 : 25 contextes
- Firepower 2130 : 30 contextes
- Firepower 2140 : 40 contextes
- Cisco Secure Firewall 3100 : 100 contextes

Par exemple, pour utiliser le maximum de 25 contextes de Firepower 1150, saisissez 23 comme nombre de contextes. Cette valeur est ajoutée à la valeur par défaut de 2.

Exemple :

```
ciscoasa(config-smart-lic)# feature context 18
```

d) (Facultatif) (Firepower 1010) Demandez la licence Security Plus pour activer le basculement.

feature security-plus

Exemple :

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) (Facultatif) (Modèles pris en charge) Demandez la licence Carrier pour l'inspection Diameter, GTP/GPRS et SCTP.

feature carrier

Exemple :

```
ciscoasa(config-smart-lic)# feature carrier
```

f) (Facultatif) Activez le cryptage renforcé. **Ne saisissez pas** cette commande si vous recevez le jeton de cryptage renforcé.

feature strong-encryption

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.



Remarque Si vous saisissez cette commande, votre appareil utilisera la licence de cryptage renforcé, qu'elle soit nécessaire ou non. Donc, à moins que vous n'ayez cette licence dans votre compte, votre compte ne sera pas conforme. Étant donné que cette licence n'est pas nécessaire lors de l'utilisation du jeton de cryptage renforcé, vous pouvez accidentellement rendre votre compte non conforme sans aucun avantage.

Exemple :

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

(Facultatif) Autres modèles : retour de la licence permanente

Si vous n'avez plus besoin d'une licence permanente (par exemple, vous retirez un ASA), vous devez officiellement renvoyer la licence à Smart Software Manager en utilisant cette procédure. Si vous ne suivez pas toutes les étapes, la licence reste dans un état utilisé et ne peut pas être libérée facilement pour être utilisée ailleurs.

Procédure

Étape 1 Sur l'ASA, générez un code de retour :

license smart reservation return

Exemple :

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

L'ASA devient immédiatement sans licence et passe à l'état d'évaluation. Si vous devez afficher de nouveau ce code, ressaisissez cette commande. Notez que si vous demandez une nouvelle licence permanente (**license smart reservation request universal**), vous ne pouvez pas réafficher ce code. Assurez-vous de capturer le code pour terminer le retour. Si la période d'évaluation a expiré, l'ASA passe à un état expiré. Pour en savoir plus sur les états de non-conformité, consultez État de non-conformité, à la page 192.

Étape 2 Affichez l'identifiant universel d'appareil (UDI) de l'ASA pour vous permettre de trouver votre instance ASA dans Smart Software Manager.

show license udi

Exemple :

```
ciscoasa# show license udi
UDI: PID:FPR-2140,SN:JAD200802RR
ciscoasa#
```

Étape 3 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Product Instances** (Instances de produit) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Product Instances** (Instances de produit) affiche tous les produits sous licence par l'UDI.

Étape 4 Recherchez l'ASA dont vous souhaitez annuler la licence, choisissez **Actions** > **Remove (Supprimer)** et saisissez le code de retour de l'ASA dans la zone. Cliquez sur **Remove Product Instance** (Supprimer l'instance de produit).

La licence permanente est renvoyée vers l'ensemble disponible.

(Autres modèles) Dérégistrer l'ASA (standard et sur site)

L'annulation de l'enregistrement de l'ASA supprime l'ASA de votre compte. Tous les droits de licence et tous les certificats de l'ASA sont supprimés. Vous souhaiterez peut-être vous désinscrire pour libérer une licence pour un nouvel ASA. Sinon, vous pouvez supprimer l'ASA du Smart Software Manager. Cette procédure s'applique aux modèles suivants :

- Firepower 1000/2100

- /3100

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 2 Cliquez sur **Unregister** (Annuler l'enregistrement).

(Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASAv (standard et sur site)

Par défaut, le certificat d'ID est automatiquement renouvelé tous les six mois et le droit de licence est renouvelé tous les 30 jours. Vous pourriez souhaiter renouveler manuellement l'enregistrement de l'un de ces éléments si vous avez une fenêtre limitée pour l'accès Internet, ou si vous apportez des modifications de licence dans Smart Software Manager, par exemple.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.

Étape 2 Pour renouveler le certificat d'ID, cliquez sur **Renew ID Certificate** (Renouveler le certificat d'ID).

Étape 3 Pour renouveler le droit de licence, cliquez sur **Renew Authorization** (Renouveler l'autorisation).

Licences par modèle

Cette section répertorie les droits de licence disponibles pour le module de sécurité ASAv et Châssis Firepower 4100/9300 ASA.

ASA virtuel

Lorsque vous définissez le niveau de débit dans la configuration ASA, cela détermine la licence demandée à Smart Software Manager. Consultez la relation suivante entre niveau de débit et licence :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

Le niveau de débit détermine également les sessions de mandataire TLS et Secure Client (services client sécurisés) maximum. Cependant, un profil de mémoire ASA virtuel inférieur limitera votre nombre réel de sessions. Par conséquent, pour déterminer vos sessions, vous devez vérifier le niveau de débit et la mémoire installée.

La mémoire de votre ASA virtuel détermine le nombre maximum de connexions et de VLAN simultanés de pare-feu et n'est pas déterminée par le niveau de débit.

Le tableau suivant présente les fonctionnalités sous licence de la gamme ASA virtuel.

Licences	Description
Licences d'autorisation	
Niveau de débit	Vous définissez le niveau de débit dans la configuration ASA. Ce niveau détermine la licence dont vous avez besoin. 100 M : ASAv5 1 G : ASAv10 2 G : ASAv30 10 G : ASAv50 20 G : ASAv100
Licences de pare-feu	
Filtre de trafic de réseau de zombies	Activé
Connexions de pare-feu, simultanées	Les connexions de pare-feu sont déterminées par la mémoire d'ASA virtuel. De 2 Go à 7,9 Go : 100 000 De 8 Go à 15,9 Go : 500 000 De 16 Go à 31,9 Go : 2 000 000 32 Go à 64 Go : 4 000 000
Transporteur	Activé

Licences	Description
Nombre total de sessions de mandataire TLS	Les sessions de mandataire TLS sont déterminées par le niveau de débit et la mémoire d'ASA virtuel. Débit de 100 M + toute mémoire : 500 Débit de 1 G + toute mémoire : 500 Débit de 2 G : • Mémoire de 2 Go à 7,9 Go : 500 • Mémoire de 8 Go+ : 1000 Débit de 10 G : • Mémoire de 2 Go à 7,9 Go : 500 • Mémoire de 8 Go à 15,9 Go : 1 000 • Mémoire de 16 Go+ : 10 000 Débit de 20 G : • Mémoire de 2 Go à 7,9 Go : 500 • Mémoire de 8 Go à 15,9 Go : 1 000 • Mémoire de 16 Go à 31,9 Go : 10 000 • Mémoire de 32 Go+ : 20 000
Licences VPN	

Licences	Description	
Homologues Secure Client (services client sécurisés)	Sans licence	Les homologues Secure Client (services client sécurisés) sont déterminés par le niveau de débit et la mémoire d'ASA virtuel. *Licence Secure Client Advantage ou Secure Client Premier facultative, maximum :* *Débit de 100 M + toute mémoire : 50* *Débit de 1 Go + toute mémoire : 250* *Débit de 2 G :* • *Mémoire de 2 Go à 7,9 Go : 250* • *Mémoire de 8 Go+ : 750* *Débit de 10 G :* • *Mémoire de 2 Go à 7,9 Go : 250* • *Mémoire de 8 Go à 15,9 Go : 750* • *Mémoire de 16 Go+ : 10 000* *Débit de 20 G :* • *Mémoire de 2 Go à 7,9 Go : 250* • *Mémoire de 8 Go à 15,9 Go : 750* • *De 16 Go à 31,9 Go : 10 000* • *Mémoire de 32 Go+ : 20 000*

Licences	Description
Autres homologues VPN	**Remarque** Les autres homologues VPN sont déterminés par le niveau de débit et la mémoire d'ASA virtuel. Débit de 100 M + toute mémoire : 50 Débit de 1 Go + toute mémoire : 250 Débit de 2 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go+ : 750 Débit de 10 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • Mémoire de 16 Go+ : 10 000 Débit de 20 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • De 16 Go à 31,9 Go : 10 000 • Mémoire de 32 Go+ : 20 000

Licences	Description
Total des homologues VPN, tous types combinés	**Remarque** Le nombre total d'homologues VPN est déterminé par le niveau de débit et la mémoire d'ASA virtuel. Débit de 100 M + toute mémoire : 50 Débit de 1 Go + toute mémoire : 250 Débit de 2 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go+ : 750 Débit de 10 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • Mémoire de 16 Go+ : 10 000 Débit de 20 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • De 16 Go à 31,9 Go : 10 000 • Mémoire de 32 Go+ : 20 000
Licences générales	
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte
Basculement	Actif/Veille
Contextes de sécurité	Aucune assistance
Mise en grappe	Activé
Nombre maximum de VLAN	Les VLAN sont déterminés par la mémoire d'ASA virtuel. De 2 Go à 7,9 Go—50 De 8 Go à 15,9 Go—200 De 16 Go à 31,9 Go—1 024 De 32 Go à 64 Go—1 024

Firepower 1010

Le tableau suivant présente les fonctionnalités sous licence du Firepower 1010.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	100 000	
Transporteur	Aucune assistance. Bien que les cartes d'inspection SCTP ne soient pas prises en charge, l'inspection avec état SCTP à l'aide d'ACL est prise en charge.	
Nombre total de sessions de mandataire TLS	4 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum : 75*
Autres homologues VPN	75	
Total des homologues VPN, tous types combinés	75	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Security Plus (basculement, équilibrage de charges VPN)	Désactivé	*Facultatif*
Contextes de sécurité	Aucune assistance.	
Mise en grappe	Aucune assistance.	
Nombre maximum de VLAN	60	

Gamme Firepower 1100

Le tableau suivant présente les fonctionnalités sous licence de la gamme Firepower 1100.

Licences	Licence Essentials
Licences de pare-feu	
Filtre de trafic de réseau de zombies	Aucune prise en charge.

Licences	Licence Essentials	
Connexions de pare-feu, simultanées	Firepower 1120 : 200 000 Firepower 1140 : 400 000 Firepower 1150 : 600 000	
Transporteur	Aucune assistance. Bien que les cartes d'inspection SCTP ne soient pas prises en charge, l'inspection avec état SCTP à l'aide d'ACL est prise en charge.	
Nombre total de sessions de mandataire TLS	Firepower 1120 : 4 000 Firepower 1140 : 8 000 Firepower 1150 : 8 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum :* *Firepower 1120 : 150* *Firepower 1140 : 400* *Firepower 1150 : 800*
Autres homologues VPN	Firepower 1120 : 150 Firepower 1140 : 400 Firepower 1150 : 800	
Total des homologues VPN, tous types combinés	Firepower 1120 : 150 Firepower 1140 : 400 Firepower 1150 : 800	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	2	*Licence facultative, maximum :* *Firepower 1120 : 5* *Firepower 1140 : 10* *Firepower 1150 : 25*
Mise en grappe	Aucune assistance.	
Nombre maximum de VLAN	1024	

Firepower Série 2100

Le tableau suivant présente les fonctionnalités sous licence de la gamme Firepower 2100.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	Firepower 2110 : 1 000 000 Firepower 2120 : 1 500 000 Firepower 2130 : 2 000 000 Firepower 2140 : 3 000 000	
Transporteur	Aucune assistance. Bien que les cartes d'inspection SCTP ne soient pas prises en charge, l'inspection avec état SCTP à l'aide d'ACL est prise en charge.	
Nombre total de sessions de mandataire TLS	Firepower 2110 : 4 000 Firepower 2120 : 8 000 Firepower 2130 : 8 000 Firepower 2140 : 10 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum :* *Firepower 2110 : 1 500* *Firepower 2120 : 3 500* *Firepower 2130 : 7 500* *Firepower 2140 : 10 000*
Autres homologues VPN	Firepower 2110 : 1 500 Firepower 2120 : 3 500 Firepower 2130 : 7 500 Firepower 2140 : 10 000	
Total des homologues VPN, tous types combinés	Firepower 2110 : 1 500 Firepower 2120 : 3 500 Firepower 2130 : 7 500 Firepower 2140 : 10 000	

Licences	Licence Essentials	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	2	*Licence facultative, maximum :* *Firepower 2110 : 25* *Firepower 2120 : 25* *Firepower 2130 : 30* *Firepower 2140 : 40*
Mise en grappe	Aucune assistance.	
Nombre maximum de VLAN	1024	

Gamme Secure Firewall 3100

Le tableau suivant présente les fonctionnalités sous licence de la gamme Secure Firewall 3100.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	Secure Firewall 3105 : 2 000 000 Secure Firewall 3110 : 2 000 000 Secure Firewall 3120 : 4 000 000 Secure Firewall 3130 : 6 000 000 Secure Firewall 3140 : 10 000 000	
Transporteur	Désactivé	*Licence facultative : opérateur*
Nombre total de sessions de mandataire TLS	Secure Firewall 3105 : 10 000 Secure Firewall 3110 : 10 000 Secure Firewall 3120 : 15 000 Secure Firewall 3130 : 15 000 Secure Firewall 3140 : 15 000	
Licences VPN		

Licences	Licence Essentials	
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum :* *Secure Firewall 3105 : 3 000* *Secure Firewall 3110 : 3 000* *Secure Firewall 3120 : 7 000* *Secure Firewall 3130 : 15 000* *Secure Firewall 3140 : 20 000*
Autres homologues VPN	Secure Firewall 3105 : 3 000 Secure Firewall 3110 : 3 000 Secure Firewall 3120 : 7 000 Secure Firewall 3130 : 15 000 Secure Firewall 3140 : 20 000	
Total des homologues VPN, tous types combinés	Secure Firewall 3105 : 3 000 Secure Firewall 3110 : 3 000 Secure Firewall 3120 : 7 000 Secure Firewall 3130 : 15 000 Secure Firewall 3140 : 20 000	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	2	*Licence facultative, maximum : 100*
Mise en grappe	Activé	
Nombre maximum de VLAN	1024	

Firepower 4100

Le tableau suivant présente les fonctionnalités sous licence du Firepower 4100.

Licences	Licence Essentials
Licences de pare-feu	
Filtre de trafic de réseau de zombies	Aucune prise en charge.

Licences	Licence Essentials	
Connexions de pare-feu, simultanées	Firepower 4112 : 10 000 000 Firepower 4115 : 15 000 000 Firepower 4125 : 25 000 000 Firepower 4145 : 40 000 000	
Transporteur	Désactivé	*Licence facultative : opérateur*
Nombre total de sessions de mandataire TLS	15 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement :* *Firepower 4112 : 10 000* *Firepower 4115 : 15 000* *Firepower 4125 : 20 000* *Firepower 4145 : 20 000*
Autres homologues VPN	Firepower 4112 : 10 000 Firepower 4115 : 15 000 Firepower 4125 : 20 000 Firepower 4145 : 20 000	
Total des homologues VPN, tous types combinés	Firepower 4112 : 10 000 Firepower 4115 : 15 000 Firepower 4125 : 20 000 Firepower 4145 : 20 000	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	10	*Licence facultative : maximum de 250*
Mise en grappe	Activé	
Nombre maximum de VLAN	1024	

Firepower 9300

Le tableau suivant présente les fonctionnalités sous licence du Firepower 9300.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	Firepower 9300 SM-56 : 60 000 000 Firepower 9300 SM-48 : 60 000 000 Firepower 9300 SM-40 : 55 000 000	
Carrier (exploitant)	Désactivé	*Licence facultative : opérateur*
Nombre total de sessions de mandataire TLS	15 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement : 20 000 maximum*
Autres homologues VPN	20 000	
Total des homologues VPN, tous types combinés	20 000	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	10	*Licence facultative : maximum de 250*
Mise en grappe	Activé	
Nombre maximum de VLAN	1024	

Supervision des licences logicielles Smart

Vous pouvez superviser les fonctionnalités, l'état et le certificat de la licence, et activer les messages de débogage.

Affichage de votre licence actuelle

Consultez l'écran suivant pour afficher votre licence :

- Accédez au volet **Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Smart Licensing (Licences Smart)** et affichez la zone **Effective Running Licenses** (Licences d'exécution effectives).

Affichage de l'état de la licence Smart

Consultez les commandes suivantes pour afficher l'état de la licence :

- **Monitoring > Properties > Smart License**

  Affiche l'état des licences logicielles Smart, la version de Smart Agent, les renseignements de l'UDI, l'état de Smart Agent, l'état de conformité globale, l'état des droits, les renseignements sur le certificat de licence et les tâches Smart Agent planifiées.

Affichage de l'UDI

Consultez la commande suivante pour afficher l'identifiant universel du produit (UDI) :

show license udi

L'exemple suivant montre l'UDI pour l'ASAv :

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

Communication avec Smart Software Manager

Cette section décrit comment votre périphérique communique avec Smart Software Manager.

Enregistrement de l'appareil et jetons

Pour chaque compte virtuel, vous pouvez créer un jeton d'enregistrement. Ce jeton est valide pendant 30 jours par défaut. Saisissez cet ID de jeton ainsi que les niveaux de droits lorsque vous déployez chaque périphérique ou lorsque vous enregistrez un périphérique existant. Vous pouvez créer un nouveau jeton si un jeton existant a expiré.

Remarque Châssis Firepower 4100/9300 : l'enregistrement du périphérique est configuré dans le châssis, et non sur le périphérique logique ASA.

Au démarrage après le déploiement, ou après avoir configuré manuellement ces paramètres sur un appareil existant, le périphérique s'enregistre auprès du Smart Software Manager. Lorsque le périphérique s'enregistre avec le jeton, le Smart Software Manager émet un certificat d'identification pour la communication entre le

périphérique et le Smart Software Manager. Ce certificat est valide pendant 1 an, mais il sera renouvelé tous les 6 mois.

Communication périodique avec le Smart Software Manager

Le périphérique communique avec Smart Software Manager tous les 30 jours. Si vous apportez des modifications à Smart Software Manager, vous pouvez actualiser l'autorisation sur le périphérique pour que les modifications prennent effet immédiatement. Vous pouvez également attendre que le périphérique communique comme planifié.

Vous pouvez éventuellement configurer un mandataire HTTP.

ASA virtuel

L'ASA virtuel doit avoir un accès Internet directement ou par l'intermédiaire d'un mandataire HTTP au moins tous les 90 jours. La communication normale de licence a lieu tous les 30 jours, mais avec le délai de grâce, votre périphérique restera conforme pendant 90 jours sans appel à Cisco. Après le délai de grâce, vous devez communiquer avec Smart Software Manager, sinon votre ASA virtuel ne sera pas conforme; l'opération n'est pas affectée par le reste.

Tous les autres modèles

L'ASA doit avoir un accès Internet directement ou par l'intermédiaire d'un mandataire HTTP au moins tous les 90 jours. La communication normale de licence a lieu tous les 30 jours, mais avec le délai de grâce, votre périphérique fonctionnera jusqu'à 90 jours sans appel à Cisco. Après le délai de grâce, vous devez communiquer avec Smart Software Manager, sinon vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales, mais le fonctionnement n'en sera pas affecté autrement.

État de non-conformité

Le périphérique peut devenir non conforme dans les situations suivantes :

- Surutilisation : le périphérique utilise plus de licences qu'il n'y en a de disponibles.
- Expiration de la licence : une licence à durée limitée a expiré.
- Absence de communication : le périphérique ne parvient pas à joindre l'autorité de licence pour une nouvelle autorisation, ce qui entraîne l'expiration de l'autorisation.

Pour vérifier si votre périphérique est dans un état de non-conformité ou s'en approche, vous devez comparer les droits actuellement utilisés par votre périphérique avec ceux de votre compte Smart.

Lorsque le périphérique n'est pas conforme, les opérations peuvent être limitées, selon le modèle :

- ASA virtuel : le système passe à un état restreint qui limite les sessions AnyConnect simultanées à deux et limite le débit total à 100 kbit/s. Cette limitation de débit garantit que le périphérique continue de fonctionner, mais avec une capacité considérablement réduite, jusqu'à ce qu'une licence valide soit installée. Ce comportement est spécifique au modèle ASA virtuel.
- Tous les autres modèles : tant que vous ne vous êtes pas enregistré auprès de l'autorité de licence, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales, mais le fonctionnement ne sera pas autrement affecté. Par exemple, les contextes existants au-dessus de la limite de licence Essentials peuvent continuer à s'exécuter et vous pouvez modifier leur configuration, mais vous ne pourrez pas ajouter un *nouveau* contexte. Si vous ne disposez pas de licences Essentials suffisantes

lors de votre première inscription, vous ne pouvez pas configurer de fonctionnalités sous licence, y compris les fonctionnalités de cryptage renforcé.

Infrastructure Smart Call Home

Par défaut, un profil Smart Call Home existe dans la configuration qui spécifie l'URL de Smart Software Manager. Vous ne pouvez pas supprimer ce profil. Notez que la seule option configurable pour le profil de licence est l'URL d'adresse de destination de Smart Software Manager. Sauf indication contraire du TAC de Cisco, vous ne devez pas modifier l'URL de Smart Software Manager.



Remarque Pour le Châssis Firepower 4100/9300 , Smart Call Home pour les licences est configuré dans le superviseur Châssis Firepower 4100/9300 , et non sur l'ASA.

Vous ne pouvez pas désactiver Smart Call Home pour les licences logicielles Smart. Par exemple, même si vous désactivez Smart Call Home à l'aide de la commande **no service call-home**, la licence logicielle Smart n'est pas désactivée.

Les autres fonctions de Smart Call Home ne sont pas activées, sauf si vous les configurez expressément.

Gestion des certificats de licence Smart

L'ASA crée automatiquement un point de confiance contenant le certificat de la CA qui a émis le certificat de serveur Smart Transport ou Smart Call Home. Pour éviter une interruption du service si la hiérarchie d'émission du certificat de serveur change, configurez la commande **Automatic Import (Importation automatique)** de l'écran **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **Trusted Certificate Pool (Ensemble de certificats de confiance)** > **Edit Trusted Certificate Pool Policy (Modifier la politique de l'ensemble de certificats de confiance)** pour activer la mise à jour automatique du groupe de certificats de confiance à des intervalles périodiques.

Le certificat de serveur reçu d'un serveur de journal système doit contenir « ServAuth » dans le champ Extended Key Usage (Utilisation de la clé étendue). Cette vérification sera effectuée uniquement pour les certificats non autosignés. Les certificats autosignés ne fournissent aucune valeur dans ce champ.



Remarque Le rechargement d'un périphérique avec un enregistrement de licence expiré depuis plus d'un an désactivera la fonctionnalité contrôlée à l'exportation. Cela peut entraîner des problèmes critiques, comme une interruption du VPN ou des scénarios de basculement avec partage de cerveau lorsque le chiffrement IPsec est activé.

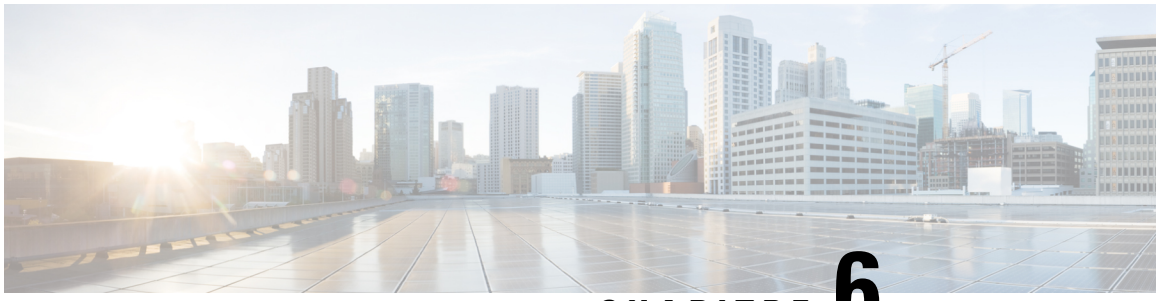
Historique des licences logicielles Smart

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de Secure Firewall 3100 pour la licence d'opérateur	9.18(1)	La licence d'opérateur permet l'inspection des protocoles Diameter, GTP/GPRS et SCTP. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
Réservation de licence permanente ASAv100	9.14(1.30)	L'ASAv100 prend désormais en charge la réservation de licence permanente à l'aide de l'ID de produit L-ASAV100SR-K9=. **Remarque :** tous les comptes ne sont pas approuvés pour la réservation de licence permanente.
Prise en charge MSLA ASA virtuel	9.13(1)	L'ASA virtuel prend en charge le programme Contrat de licences de services gérés (MSLA) de Cisco, une structure d'octroi de licences et d'utilisation de logiciels conçue pour les clients et les partenaires de Cisco qui offrent des services gérés de logiciels à des tiers. MSLA est une nouvelle forme de licence Smart dans laquelle l'agent de licence Smart assure le suivi de l'utilisation des droits de licence par unités de temps. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
Licences flexibles ASA virtuel	9.13(1)	Les licences flexibles sont une nouvelle forme de licences Smart dans lesquelles n'importe quelle licence ASA virtuel peut désormais être utilisée sur n'importe quelle configuration de vCPU/mémoire ASA virtuel prise en charge. Les limites de session pour Secure Client (services client sécurisés) et le mandataire TLS seront déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée plutôt que par une limite de plateforme liée à un type de modèle. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)**.
Modifications de licence pour les paires de basculement sur le Châssis Firepower 4100/9300	9.7(1)	Seule l'unité active demande les droits de licence. Auparavant, les deux unités demandaient des droits de licence. Pris en charge par FXOS 2.1.1.
Réservation de licence permanente pour l'amélioration des chaînes courtes d'ASA virtuel	9.6(2)	En raison d'une mise à jour de Smart Agent (vers 1.6.4), les codes de demande et d'autorisation utilisent désormais des chaînes plus courtes. Nous n'avons pas modifié d'écrans.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge du serveur satellite pour l'ASA virtuel	9.6(2)	Si vos périphériques ne peuvent pas accéder à Internet pour des raisons de sécurité, vous pouvez éventuellement installer un serveur satellite Smart Software Manager local en tant que machine virtuelle (VM). Nous n'avons pas modifié d'écrans.
Réservation de licence permanente pour l'ASA sur le Châssis Firepower 4100/9300	9.6(2)	Pour les environnements hautement sécurisés où la communication avec Cisco Smart Software Manager n'est pas autorisée, vous pouvez demander une licence permanente pour l'ASA sur le Firepower 9300 et le Firepower 4100. Tous les droits de licence disponibles sont inclus dans la licence permanente, y compris les licences de niveau standard, de cryptage renforcé (le cas échéant), de contextes de sécurité et d'opérateur. FXOS 2.0.1 est nécessaire. Toute la configuration est effectuée sur le Châssis Firepower 4100/9300 ; aucune configuration n'est requise sur l'ASA.
Réservation de licence permanente pour l'ASA virtuel	9.5(2.200) 9.6(2)	Pour les environnements hautement sécurisés où la communication avec Cisco Smart Software Manager n'est pas autorisée, vous pouvez demander une licence permanente pour l'ASA virtuel. Dans la version 9.6(2), nous avons également ajouté la prise en charge de cette fonctionnalité pour l'ASA virtuel sur Amazon Web Services. Cette fonctionnalité n'est pas prise en charge pour Microsoft Azure. Nous avons introduit les commandes suivantes : **license smart reservation, license smart reservation cancel, license smart reservation install, license smart reservation request universal, license smart reservation return** ASDM n'est pas pris en charge.
Mise à niveau de Smart Agent vers la version 1.6	9.5(2.200) 9.6(2)	Smart Agent a été mis à niveau de la version 1.1 à la version 1.6. Cette mise à niveau prend en charge la réservation de licences permanentes et prend également en charge la définition du droit de licence de cryptage renforcé (3DES/AES) en fonction de l'autorisation définie dans votre compte de licence. **Remarque** Si vous rétrogradez à partir de la version 9.5(2.200), l'ASA virtuel ne conserve pas l'état d'enregistrement de la licence. Vous devez vous réenregistrer à l'aide de la commande **: page Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Smart Licensing (Licences Smart)** et utilisez l'option **Force registration** (Forcer l'enregistrement); obtenir le jeton d'identification auprès de Smart Software Manager. Nous n'avons pas modifié d'écrans.

Nom de la caractéristique	Versions de plateforme	Description
Licence de cryptage renforcé (3DES) automatiquement appliquée pour l'ASA sur le Firepower 9300	9.5(2.1)	Pour les utilisateurs de Cisco Smart Software Manager standard, la licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement sur le châssis. Dans ce cas-là, aucune action supplémentaire n'est requise sur le Firepower 9300. **Remarque** Si vous utilisez le déploiement satellite du Smart Software Manager, pour utiliser ASDM et d'autres fonctionnalités de cryptage renforcé, après avoir déployé l'ASA, vous devez activer la licence de cryptage renforcé (3DES) à l'aide de l'interface de ligne de commande d'ASA. Cette fonctionnalité nécessite FXOS 1.1.3. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des dispositifs)** > **Licensing (Licence)** > **Smart License (Licence Smart)**
Validation du certificat Smart Call Home/de licence Smart si la hiérarchie d'émission du certificat de serveur change	9.5(2)	La licence Smart utilise l'infrastructure Smart Call Home. Lorsque l'ASA configure pour la première fois les rapports anonymes de Smart Call Home en arrière-plan, il crée automatiquement un point de confiance contenant le certificat de la CA qui a émis le certificat de serveur Smart Call Home. L'ASA prend désormais en charge la validation du certificat si la hiérarchie d'émission du certificat de serveur change; vous pouvez activer la mise à jour automatique du groupe de confiance à des intervalles périodiques. Nous avons modifié l'écran suivant : **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **Trusted Certificate Pool (Groupe de certificats de confiance)** > **Edit Trusted Certificate Pool Policy (Modifier la politique du groupe de certificats de confiance)**
Licence de transporteur	9.5(2)	La nouvelle licence de transporteur remplace la licence GTP/GPRS existante et comprend également la prise en charge de l'inspection SCTP et Diameter. Pour l'ASA sur le châssis Firepower 9300, la commande **feature mobile-sp** passera automatiquement à la commande **feature carrier**. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des dispositifs)** > **Licensing (Licence)** > **Smart License (Licence Smart)**
Licences logicielles Cisco Smart pour l'ASA sur le Firepower 9300	9.4(1.150)	Nous avons introduit les licences logicielles Cisco Smart pour l'ASA sur le Firepower 9300 Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des dispositifs)** > **Licensing (Licence)** > **Smart License (Licence Smart)**

Nom de la caractéristique	Versions de plateforme	Description
Licence logicielle Smart de Cisco pour l'ASA virtuel	9.3(2)	Smart Software Licensing vous permet d'acheter et de gérer un ensemble de licences. Contrairement aux licences PAK, les licences Smart ne sont pas liées à un numéro de série ou à une clé de licence spécifique. Vous pouvez facilement déployer ou retirer des ASA virtuel sans avoir à gérer la clé de licence de chaque unité. Smart Software Licensing vous permet également de consulter votre utilisation et vos besoins en licences en un clin d'œil. Nous avons introduit ou modifié les écrans suivants : **Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Smart License Configuration (Configuration de la licence Smart) > Device Management (Gestion des périphériques) > Smart Call-Home Monitoring (Surveillance Smart Call-Home) > Properties (Propriétés) > Smart License (Licence Smart)**



CHAPITRE 6

Périphériques logiques pour le Firepower 4100/9300

Firepower 4100/9300 est une plateforme de sécurité flexible sur laquelle vous pouvez installer un ou plusieurs *périphériques logiques*. Ce chapitre décrit la configuration de l'interface de base et comment ajouter un périphérique logique autonome ou à haute accessibilité à l'aide de Firewall Chassis Manager. Pour ajouter un périphérique logique en grappe, consultez Grappe ASA pour le Firepower 4100/9300, à la page 451. Pour utiliser l'interface de ligne de commande de FXOS, consultez le guide de configuration de l'interface de ligne de commande FXOS. Pour des procédures FXOS et un dépannage plus avancés, consultez le guide de configuration FXOS.

- À propos des interfaces, à la page 199
- À propos des périphériques logiques, à la page 202
- Exigences et conditions préalables pour les combinaisons matérielles et logicielles , à la page 203
- Lignes directrices et limites relatives aux périphériques logiques, à la page 204
- Interfaces de configuration, à la page 205
- Configurer les périphériques logiques, à la page 209
- Historique des périphériques logiques, à la page 216

À propos des interfaces

Le châssis Firepower 4100/9300 prend en charge les interfaces physiques et les interfaces EtherChannel (canal de port). Les interfaces EtherChannel peuvent comprendre jusqu'à 16 interfaces membres du même type.

Interface de gestion de châssis

L'interface de gestionnaire de châssis est utilisée pour la gestion du châssis FXOS par SSH ou Firewall Chassis Manager. Cette interface apparaît en haut de l'onglet **Interfaces** en tant que **MGMT**, et vous ne pouvez activer ou désactiver cette interface que dans l'onglet **Interfaces**. Cette interface est distincte de l'interface de type gestion (mgmt) que vous affectez aux périphériques logiques pour la gestion des applications.

Pour configurer les paramètres de cette interface, vous devez les configurer à partir de l'interface de ligne de commande. Pour afficher des informations sur cette interface dans l'interface de ligne de commande FXOS, connectez-vous à la gestion locale et affichez le port de gestion :

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

Notez que l'interface de gestion du châssis reste active même si le câble physique ou le module SFP est débranché ou que la commande **mgmt-port shut** est exécutée ou si le périphérique logique est hors-ligne.

Remarque L'interface de gestion de châssis ne prend pas en charge les trames étendues.

Types d'interface

Les interfaces physiques et les interfaces EtherChannel (canal de port) peuvent être de l'un des types suivants :

- Données : à utiliser pour les données normales. Les interfaces de données ne peuvent pas être mises en commun entre les périphériques logiques, et les périphériques logiques ne peuvent pas communiquer avec d'autres périphériques logiques par le fond de panier Pour le trafic sur les interfaces de données, tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre périphérique logique.
- Data-sharing (partage de données) : à utiliser pour les données normales. Pris en charge uniquement avec les instances de conteneur, ces interfaces de données peuvent être partagées par un ou plusieurs dispositifs logiques/Instances de conteneur (Firewall Threat Defense-utilisant-Firewall Management Center seulement).
- Gestion : permet de gérer les instances d'application. Ces interfaces peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface. Vous ne pouvez affecter qu'une seule interface de gestion par périphérique logique. En fonction de votre application et de votre gestionnaire, vous pouvez ultérieurement activer la gestion à partir d'une interface de données; mais vous devez attribuer une interface de gestion au dispositif logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données.Pour en savoir plus sur l'interface de gestion de châssis distincte, consultez Interface de gestion de châssis, à la page 199.

Remarque La modification de l'interface de gestion entraînera le redémarrage du périphérique logique. Par exemple, une gestion des modifications de e1/1 à e1/2 entraînera le redémarrage du périphérique logique pour appliquer la nouvelle gestion.

- Créer un événement— Sert d'interface de gestion secondaire pour les périphériques Firewall Threat Defense-using- (en usage) Firewall Management Center.

Remarque Une interface Ethernet virtuelle est attribuée lors de l'installation de chaque instance applicative. Si l'application n'utilise pas d'interface événementielle, l'interface virtuelle sera dans un état "admin down".

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster (grappe) : à utiliser comme liaison de commande de grappe pour un périphérique logique en grappe. Par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48. Le type de grappe est uniquement pris en charge sur les interfaces EtherChannel.

Reportez-vous à la table suivante pour la prise en charge des types d'interface pour les demandes Firewall Threat Defense et ASA dans les déploiements autonomes et en grappe.

Tableau 9 : Prise en charge des types d'interface

Application		Données	Données : sous-interface	Partage de données	Partage de données : sous-interface	Gestion	Créer des événements	Grappe (EtherChannel uniquement)	Grappe : sous-interface
Firewall Threat Defense	Instance native autonome	**Oui**	—	—	—	**Oui**	**Oui**	—	—
	Instance de conteneur autonome	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	—	—
	Instance native de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	**Oui**	**Oui**	—
	Instance de conteneur de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	**Oui**	**Oui**	**Oui**
ASA	Instance native autonome	**Oui**	—	—	—	**Oui**	—	**Oui**	—
	Instance native de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	—	**Oui**	—

Interfaces FXOS par rapport aux interfaces d'application

Le Firepower 4100/9300 gère les paramètres Ethernet de base des interfaces physiques et les interfaces EtherChannel (canal de port). Dans l'application, vous configurez les paramètres de niveau supérieur. Par

exemple, vous pouvez uniquement créer des EtherChannels dans FXOS; mais vous pouvez attribuer une adresse IP à l'EtherChannel dans l'application.

Les sections suivantes décrivent l'interaction entre FXOS et l'application pour les interfaces.

Sous-interfaces VLAN

Pour tous les périphériques logiques, vous pouvez créer des sous-interfaces VLAN dans l'application.

États indépendants de l'interface dans le châssis et dans l'application

Vous pouvez activer et désactiver administrativement les interfaces dans le châssis et dans l'application. Pour qu'une interface soit opérationnelle, elle doit être activée dans les deux systèmes d'exploitation. Étant donné que l'état de l'interface est contrôlé indépendamment, il se peut que vous ayez une incompatibilité entre le châssis et l'application.

À propos des périphériques logiques

Un périphérique logique vous permet d'exécuter une instance d'application (ASA ou Firewall Threat Defense) ainsi qu'une application de décochage facultative (Radware DefensePro) pour former une chaîne de services.

Lorsque vous ajoutez un périphérique logique, vous définissez également le type et la version de l'instance d'application, vous affectez des interfaces et vous configurez les paramètres de démarrage qui sont transmis à la configuration de l'application.

Remarque Pour Firepower 9300, vous pouvez installer différents types d'applications (ASA et Firewall Threat Defense) sur des modules distincts du châssis. Vous pouvez également exécuter différentes versions d'un type d'instance d'application sur des modules distincts.

Périphériques logiques autonomes et en grappe

Vous pouvez ajouter les types d'unités logiques suivants :

- Autonome : un périphérique logique autonome fonctionne comme une unité autonome ou comme une unité dans une paire à haute disponibilité.
- Grappe : un appareil logique en grappe vous permet de regrouper plusieurs unités ensemble, offrant toute la commodité d'un seul appareil (gestion, intégration dans un réseau) tout en obtenant le débit accru et la redondance de plusieurs périphériques. Les périphériques à modules multiples, comme le périphérique Firepower 9300, prennent en charge la mise en grappe à l'intérieur des châssis. Pour le périphérique Firepower 9300, les trois modules doivent faire partie de la grappe, à la fois pour les instances natives et de conteneur.

Exigences et conditions préalables pour les combinaisons matérielles et logicielles

Le Firepower 4100/9300 prend en charge plusieurs modèles, modules de sécurité, types d'applications, et de haute disponibilité et d'évolutivité. Consultez les exigences suivantes pour connaître les combinaisons autorisées.

Exigences du périphérique Firepower 9300

L'appareil Firepower 9300 comprend 3 logements pour module de sécurité et plusieurs types de modules de sécurité. Consultez les exigences suivantes :

- Security Module Types (types de modules de sécurité) : Vous pouvez installer des modules de différents types dans le périphérique Firepower 9300. Par exemple, vous pouvez installer le SM-48 comme module 1, le SM-40 comme module 2 et le SM-56 comme module 3.
- Instances natives et de conteneur : lorsque vous installez une instance de conteneur sur un module de sécurité, ce module ne peut prendre en charge que d'autres instances de conteneur. Une instance native utilise toutes les ressources d'un module, vous ne pouvez donc installer qu'une seule instance native sur un module. Vous pouvez utiliser des instances natives sur certains modules et des instances de conteneur sur les autres modules. Par exemple, vous pouvez installer une instance native sur le module 1 et le module 2, mais des instances de conteneur sur le module 3.
- Mise en grappe : tous les modules de sécurité de la grappe, qu'elle soit intra-châssis ou inter-châssis, doivent être du même type. Vous pouvez avoir différentes quantités de modules de sécurité installés dans chaque châssis, bien que tous les modules présents dans le châssis doivent appartenir à la grappe, y compris les logements vides. Par exemple, vous pouvez installer 2 SM-40 dans le châssis 1 et 3 SM-40 dans le châssis 2. Vous ne pouvez pas utiliser la mise en grappe si vous installez 1 SM-48 et 2 SM-40 dans le même châssis.
- High Availability (haute disponibilité) : la haute disponibilité est prise en charge uniquement entre les modules de même type sur le périphérique Firepower 9300. Cependant, les deux châssis peuvent comprendre des modules mixtes. Par exemple, chaque châssis a un SM-40, SM-48 et SM-56. Vous pouvez créer des paires à haute disponibilité entre les modules SM-40, entre les modules SM-48 et entre les modules SM-56.
- Types d'applications ASA et Firewall Threat Defense :Vous pouvez installer différents types d'applications sur des modules distincts dans le châssis. Par exemple, vous pouvez installer ASA sur le module 1 et le module 2, et Firewall Threat Defense sur le module 3.
- Versions ASA ou Firewall Threat Defense : vous pouvez exécuter différentes versions d'un type d'instance d'application sur des modules distincts ou en tant qu'instances de conteneur distinctes sur le même module. Par exemple, vous pouvez installer Firewall Threat Defense 6.3 sur le module 1, Firewall Threat Defense 6.4 sur le module 2 et Firewall Threat Defense 6.5 sur le module 3.

Exigences du périphérique Firepower 4100

L'appareil Firepower 4100 est offert en plusieurs modèles. Consultez les exigences suivantes :

- Instances natives et de conteneur : lorsque vous installez une instance de conteneur sur une Firepower 4100, cet appareil ne peut prendre en charge que d'autres instances de conteneur. Une instance native

utilise toutes les ressources d'un périphérique, vous ne pouvez donc installer qu'une seule instance native sur le périphérique.

- Mise en grappe : tous les châssis de la grappe doivent être du même modèle.
- Haute disponibilité : la haute disponibilité est uniquement prise en charge entre les modèles du même type.
- Types d'application ASA et Firewall Threat Defense : Firepower 4100 ne peut exécuter qu'un seul type d'application.

Lignes directrices et limites relatives aux périphériques logiques

Consultez les sections suivantes pour connaître les instructions et les limites.

Lignes directrices et limites des interfaces

Adresses MAC par défaut

Les attributions d'adresses MAC par défaut dépendent du type d'interface.

- Interfaces physiques : l'interface physique utilise l'adresse MAC gravée.
- EtherChannels : Pour un EtherChannel, toutes les interfaces du groupe de canaux partagent la même adresse MAC. Cette fonction rend l'EtherChannel transparent pour les applications et les utilisateurs du réseau, car ils ne voient qu'une seule connexion logique; ils n'ont aucune connaissance des liens individuels. L'interface du canal de port utilise une adresse MAC unique provenant d'un pool; L'appartenance à l'interface n'affecte pas l'adresse MAC.

Lignes directrices et limites générales

Mode pare-feu

Vous pouvez définir le mode de pare-feu routé ou transparent dans la configuration de démarrage des Firewall Threat Defense et ASA.

Haute disponibilité

- Configurez la haute disponibilité dans la configuration de l'application.
- Vous pouvez utiliser n'importe quelle interface de données comme liens de basculement et d'état.Les interfaces de partage de données ne sont pas prises en charge.

Mode contexte

- Activez le mode de contexte multiple dans l'ASA après le déploiement.

Exigences et prérequis pour la haute accessibilité

- Les deux unités d'une configuration de basculement à haute accessibilité doivent :
  - Être sur un châssis séparé; la haute accessibilité intra-châssis pour le Firepower 9300 n'est pas prise en charge.
  - être du même modèle.
  - Avoir les mêmes interfaces que celles des périphériques logiques à haute accessibilité.
  - Avoir le même nombre et les mêmes types d'interfaces. Toutes les interfaces doivent être préconfigurées de manière identique dans FXOS avant que vous activiez la haute accessibilité.
- La haute accessibilité est uniquement prise en charge entre les modules de même type sur le Firepower 9300; toutefois, les deux châssis peuvent inclure des modules mixtes. Par exemple, chaque châssis a un SM-56, SM-48 et SM-40. Vous pouvez créer des paires à haute accessibilité entre les modules SM-56, entre les modules SM-48 et entre les modules SM-40.
- Pour les autres exigences du système en matière de haute accessibilité, consultez Configuration système requise Basculement, à la page 294.

Interfaces de configuration

Par défaut, les interfaces physiques sont désactivées. Vous pouvez activer les interfaces, ajouter des canaux EtherChannels, et modifier les propriétés de l'interface et .

Remarque Si vous supprimez une interface dans FXOS (p. ex., si vous supprimez un module de réseau, supprimez un canal EtherChannel ou réaffectez une interface à un canal EtherChannel), la configuration ASA conserve les commandes d'origine afin que vous puissiez effectuer les ajustements nécessaires; retirer une interface de la configuration peut avoir des effets considérables. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation ASA.

Activer ou désactiver une interface

Vous pouvez modifier l' **état d'administration** de chaque interface pour l'activer ou la désactiver. Par défaut, les interfaces physiques sont désactivées.

Procédure

Étape 1 Choisissez **Interfaces** pour ouvrir la page des interfaces.

La page Interfaces présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Pour activer l'interface, cliquez sur le bouton désactivé **Curseur désactivé** () pour qu'il devienne activé **Curseur activé** ().

Cliquez sur **Yes** (oui) pour confirmer la modification. L'interface correspondante dans la représentation visuelle passe du gris au vert.

Étape 3 Pour désactiver l'interface, cliquez sur le **Curseur activé** () activé pour qu'elle devienne désactivée **Curseur désactivé** ().

Cliquez sur **Yes** (oui) pour confirmer la modification. L'interface correspondante dans la représentation visuelle passe du vert au gris.

Configurer une interface physique

Vous pouvez physiquement activer et désactiver les interfaces, ainsi que définir la vitesse d'interface et le mode duplex. Pour utiliser une interface, elle doit être physiquement activée dans FXOS et logiquement activée dans l'application.

Remarque

- Dans le cas de QSFPH40G-CUxM, la négociation automatique est toujours activée par défaut et vous ne pouvez pas la désactiver.
- Si vous remplacez un module SFP sur un port par un module SFP différent, la vitesse, les conditions de duplex et la négociation automatique de l'interface ne sont pas mises à jour automatiquement. Vous devez reconfigurer manuellement l'interface.

Avant de commencer

- Les interfaces qui sont déjà membres d'un EtherChannel ne peuvent pas être modifiées individuellement. Assurez-vous de configurer les paramètres avant de les ajouter au canal EtherChannel.

Procédure

Étape 1 Choisissez **Interfaces** pour ouvrir la page des interfaces.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Edit** (modifier) dans la ligne de l'interface à modifier pour ouvrir la boîte de dialogue **Edit Interface** (modifier l'interface).

Étape 3 Activez l'interface en cochant la case **Enable** (activer). Désactivez l'interface en décochant la case **Enable** (activer).

Étape 4 Choisissez le **Type** d'interface :

Consultez Types d'interface, à la page 200 pour obtenir plus de détails sur l'utilisation de ce type d'interface.

- **Data** (Données)
- **Gestion**
- **Cluster (grappe)** : Ne choisissez pas le type **Cluster**; par défaut, la liaison de commande de grappe est automatiquement créée sur le port-canal 48.

Étape 5 (Facultatif) Choisissez la vitesse de l'interface dans la liste déroulante **Speed**.

Étape 6 (Facultatif) Si votre interface prend en charge la négociation automatique (**Auto Negotiation**), cliquez sur le bouton radio **Yes** (oui) ou **No** (non).

Si un commutateur homologue se connectant au port sur un câble 50G ne prend pas en charge la négociation automatique, assurez-vous de désactiver la négociation automatique sur le commutateur et l'interface de plateforme. Par exemple, N9K-C93400LD-H1 ne prend pas en charge la négociation automatique sur un câble 50G. Par conséquent, pour que le port soit connecté, vous devez désactiver la négociation automatique par défaut sur la plateforme et le commutateur.

Étape 7 (Facultatif) Choisissez le duplex de l'interface dans la liste déroulante **Duplex**.

Étape 8 (Facultatif) Configurez explicitement le **Délai anti-rebond (ms)**. Saisissez une valeur comprise entre 0 et 15 000 milli-secondes.

Remarque La configuration du délai antirebond n'est pas prise en charge sur les interfaces 1G.

Étape 9 Cliquez sur **OK**.

Ajouter un canal EtherChannel (canal de port)

Un EtherChannel (également appelé canal de port) peut inclure jusqu'à 16 interfaces membres de même type de support et de capacité, et doit être réglé à la même vitesse et au même duplex. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité. Le protocole LACP (Link Aggregation Control Protocol) agrège les interfaces en échangeant les LACPDU (Link Aggregation Control Protocol Data Unit) entre deux périphériques réseau.

Vous pouvez configurer chaque interface physique de données dans un EtherChannel pour qu'elle soit :

- Actif : envoie et reçoit les mises à jour du protocole LACP. Un EtherChannel actif peut établir une connectivité avec un EtherChannel actif ou passif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.
- Activé : l'EtherChannel est toujours activé et le protocole LACP n'est pas utilisé. Un EtherChannel « activé » ne peut établir une connexion qu'avec un autre EtherChannel « activé ».

Remarque Cela peut prendre jusqu'à trois minutes à un EtherChannel de revenir à l'état opérationnel si vous faites passer son mode de On (Activé) à Actif ou de Actif à Activé.

Les interfaces sans données ne prennent en charge que le mode actif.

Le protocole LACP coordonne l'ajout et la suppression automatiques des liens vers l'EtherChannel sans l'intervention de l'utilisateur. Il gère également les erreurs de configuration et vérifie que les deux extrémités des interfaces membres sont connectées au groupe de canaux approprié. Le mode « Activé» ne peut pas utiliser les interfaces en veille dans le groupe de canaux lorsqu'une interface tombe en panne et que la connectivité et les configurations ne sont pas vérifiées.

Lorsque Firepower 4100/9300 crée un EtherChannel, l'EtherChannel reste dans un état **Suspendu** pour le mode LACP actif ou à l'arrêt pour le mode LACP **activé** jusqu'à ce que vous l'affectiez à un périphérique logique, même si le lien physique est actif. L'EtherChannel sortira de l'état **Suspendu** dans les situations suivantes :

- L'EtherChannel est ajouté en tant qu'interface de données ou de gestion pour un périphérique logique autonome
- L'EtherChannel est ajouté en tant qu'interface de gestion ou liaison de commande de grappe pour un périphérique logique qui fait partie d'une grappe
- L'EtherChannel est ajouté en tant qu'interface de données pour un périphérique logique qui fait partie d'une grappe et au moins une unité a rejoint la grappe

Notez que l'EtherChannel ne s'affiche pas tant que vous ne l'avez pas affecté à un périphérique logique. Si l'EtherChannel est retiré de l'unité logique ou si l'unité logique est supprimée, il repasse à l'état **Suspendu** ou **Inactif**.

Procédure

Étape 1 Choisissez **Interfaces** pour ouvrir la page des interfaces.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Add Port Channel** (ajouter un canal de port) au-dessus du tableau des interfaces pour ouvrir la boîte de dialogue **Add Port Channel** (ajouter un canal de port).

Étape 3 Dans le champ **Port Channel ID**, entrez un numéro identifiant le canal de port. Les valeurs valides sont comprises entre 1 et 47.

Le canal de port 48 est réservé pour la liaison de commande de grappe lorsque vous déployez un périphérique logique en grappe. Si vous ne souhaitez pas utiliser le canal de port 48 pour la liaison de commande de grappe, vous pouvez le supprimer et configurer un EtherChannel de type grappe avec un ID différent.Vous pouvez ajouter plusieurs EtherChannels de type grappe et ajouter des sous-interfaces VLAN à utiliser avec la mise en grappe à instances multiples. Pour la mise en grappe intra-châssis, n'affectez aucune interface à la grappe EtherChannel.

Étape 4 Cochez la case **Enable** pour activer le canal de port. Cochez la case **Disable** pour désactiver le canal de port.

Étape 5 Choisissez le **Type** d'interface :

Consultez Types d'interface, à la page 200 pour obtenir plus de détails sur l'utilisation de ce type d'interface.

- **Data** (Données)
- **Gestion**
- **Cluster** (Grappe)

Étape 6 Définissez la **vitesse d'administration** requise pour les interfaces membres dans la liste déroulante.

Si vous ajoutez une interface membre qui n'a pas la vitesse spécifiée, elle ne pourra pas rejoindre le canal de port.

Étape 7 Pour les données , choisissez le **mode**du canal de port LACP , **Actif** ou **Activé**.

Pour les interfaces sans données, le mode est toujours actif.

Étape 8 Définissez le **duplex d'administration** requis pour les interfaces membres, soit **le duplex intégral** ou **semi-duplex**.

Si vous ajoutez une interface membre configurée avec le duplex précisé, elle ne rejoindra pas le canal de port.

Étape 9 Pour ajouter une interface au canal de port, sélectionnez l'interface dans la liste des **interfaces disponibles** et cliquez sur **Add Interface** (ajouter une interface) pour déplacer l'interface vers la liste d'ID de membre.

Vous pouvez ajouter jusqu'à 16 interfaces du même type et de la même vitesse. Les interfaces membres doivent être réglées à la même vitesse et au même duplex et doivent correspondre à la vitesse et au duplex que vous avez configurés pour ce canal de port. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité.

Astuces Vous pouvez ajouter plusieurs interfaces en même temps. Pour sélectionner plusieurs interfaces, cliquez sur les interfaces souhaitées tout en maintenant la touche **Ctrl** enfoncée. Pour sélectionner une plage d'interfaces, sélectionnez la première interface de la plage, puis, tout en maintenant la touche **Maj** (Shift) enfoncée, cliquez pour sélectionner la dernière interface de la plage.

Étape 10 Pour supprimer une interface du canal de port, cliquez sur le bouton **Supprimer** à droite de l'interface dans la liste des ID de membre.

Étape 11 Cliquez sur **OK**.

Configurer les périphériques logiques

Ajoutez un périphérique logique autonome ou une paire à haute disponibilité sur le Châssis Firepower 4100/9300 .

Pour la mise en grappe, consultez #unique_274.

Ajouter un ASA autonome

Les périphériques logiques autonomes fonctionnent seuls ou dans une paire haute disponibilité. Sur Firepower 9300 avec plusieurs modules de sécurité, vous pouvez déployer une grappe ou des appareils autonomes. La grappe doit utiliser tous les modules. Par conséquent, vous ne pouvez pas combiner une grappe à deux modules et un seul périphérique autonome.

Vous pouvez déployer un ASA routé ou transparent en mode pare-feu à partir de Châssis Firepower 4100/9300 .

Pour le mode à contextes multiples, vous devez d'abord déployer le périphérique logique, puis activer le mode à contextes multiples dans l'application ASA.

Avant de commencer

- Téléchargez l'image de l'application que vous souhaitez utiliser pour le périphérique logique à partir de Cisco.com), puis chargez cette image sur Firepower 4100/9300.

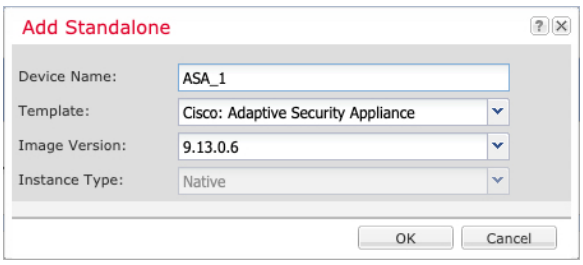
Remarque Pour Firepower 9300, vous pouvez installer différents types d'applications (ASA et Firewall Threat Defense) sur des modules distincts du châssis. Vous pouvez également exécuter différentes versions d'un type d'instance d'application sur des modules distincts.

- Configurez une interface de gestion à utiliser avec le périphérique logique. L'interface de gestion est requise. Notez que cette interface de gestion n'est pas la même que le port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis (et qui apparaît en haut de l'onglet **Interfaces** comme **MGMT**).
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce périphérique
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - Adresse IP de la passerelle

Procédure

Étape 1 Choisissez **Logical Devices** (périphériques logiques).

Étape 2 Cliquez sur **Add** > **Standalone (Ajouter un périphérique autonome)** , puis définissez les paramètres suivants :



a) Indiquez un nom de périphérique (**Device Name**).

Ce nom est utilisé par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de périphérique utilisé dans la configuration de l'application.



Remarque Vous ne pouvez pas modifier ce nom après avoir ajouté le périphérique logique.

b) pour le **Template** (modèle), choisissez **Cisco: Adaptive Security Appliance** (Cisco : Appareil de sécurité adaptable).
c) Choisissez la version de l'image (**Image Version**).
d) Cliquez sur **OK**.

Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du périphérique).

Étape 3 Développez la zone des ports de données (**Data Ports**), puis cliquez sur chaque port que vous souhaitez affecter au périphérique.

Vous ne pouvez attribuer que des interfaces de données que vous avez préalablement activées sur la page **Interfaces**. Vous activerez et configurerez ultérieurement ces interfaces dans l'ASA, y compris la définition des adresses IP.

Étape 4 Cliquez sur l'icône de périphérique au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 5 Dans la page des informations générales (**General Information**), procédez comme suit :

a) (Pour Firepower 9300) Sous **Security Module Selection** (sélection du module de sécurité), cliquez sur le module de sécurité que vous souhaitez utiliser pour ce périphérique logique.
b) Choisissez l'interface de gestion (**Management Interface**).

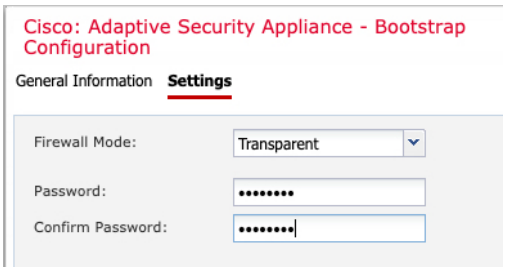
Cette interface est utilisée pour gérer le périphérique logique. Cette interface est distincte du port de gestion du châssis.

c) Choisissez le type d'adresse de l'interface de gestion (**Address Type**) : **IPv4 only** (IPv4 seulement), **IPv6 only** (IPv6 seulement), ou **IPv4 and IPv6** (IPv4 et IPv6).
d) Configurez l'adresse IP de gestion (**Management IP**).

Définissez une adresse IP unique pour cette interface.

e) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).
f) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 6 Cliquez sur l'onglet **Settings** (Paramètres).



Étape 7 Choisissez le mode du pare-feu (**Firewall Mode**) : **Transparent** ou **Routed** (routage).

En mode routage, l'ASA est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

Étape 8 Saisissez et confirmez un mot de **passe** pour l'utilisateur admin et pour le mot de passe d'activation.

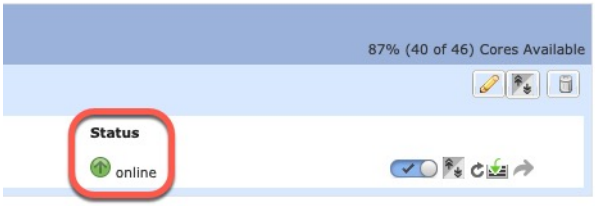
L'utilisateur/mot de passe administrateur ASA préconfigurés et le mot de passe d'activation sont utiles pour la récupération du mot de passe. si vous avez un accès FXOS, vous pouvez réinitialiser le mot de passe de l'utilisateur admin et le mot de passe d'activation si vous l'oubliez.

Étape 9 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 10 Cliquez sur **Save** (Enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez l'état du nouveau périphérique logique dans la page **Logical Devices**. Lorsque le périphérique logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la politique de sécurité dans l'application.





Étape 11 Consultez le guide de configuration ASA pour commencer à configurer votre politique de sécurité.

Ajouter une paire à haute disponibilité

La haute accessibilité ou Firewall Threat DefenseASA (également appelée basculement) est configurée dans l'application, pas dans FXOS. Toutefois, pour préparer votre châssis à la haute disponibilité, consultez les étapes suivantes.

Avant de commencer

Consultez la section Configuration système requise Basculement, à la page 294.

Procédure

Étape 1 Attribuez les mêmes interfaces à chaque périphérique logique.

Étape 2 Attribuez une ou deux interfaces de données au basculement et à l'état des liens.

Ces interfaces échangent le trafic à haute disponibilité entre les deux châssis. Nous vous recommandons d'utiliser une interface de données de 10 Go pour un basculement et une liaison d'état combinés. Si vous avez des interfaces disponibles, vous pouvez utiliser des liaisons de basculement et d'état distincts; le lien d'état nécessite le plus de bande passante. Vous ne pouvez pas utiliser l'interface de type de gestion pour la liaison de basculement ou d'état. Nous vous recommandons d'utiliser un commutateur entre les châssis, afin qu'aucun autre périphérique ne se trouve sur le même segment de réseau que les interfaces de basculement.

Étape 3 Activez la haute disponibilité sur les périphériques logiques. Consultez Basculement pour la haute disponibilité, à la page 293.

Étape 4 Si vous modifiez les interfaces après avoir activé la haute disponibilité, modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active.

Remarque Dans le cas de l'ASA, si vous supprimez une interface dans FXOS (p. ex., si vous supprimez un module de réseau, supprimez un canal EtherChannel ou réaffectez une interface à un canal EtherChannel), la configuration ASA conserve les commandes d'origine afin que vous puissiez effectuer les ajustements nécessaires; retirer une interface de la configuration peut avoir des effets considérables. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation de l'ASA.

Modifier une interface sur un périphérique logique ASA

Vous pouvez allouer, annuler l'allocation ou remplacer une interface de gestion sur un périphérique logique ASA. ASDM détecte automatiquement les nouvelles interfaces.

L'ajout d'une nouvelle interface ou la suppression d'une interface inutilisée a une incidence minime sur la configuration de l'ASA. Cependant, si vous supprimez une interface allouée dans FXOS (par exemple, si vous supprimez un module de réseau, supprimez un EtherChannel ou réaffectez une interface allouée à un EtherChannel) et que l'interface est utilisée dans votre politique de sécurité, la suppression aura une incidence sur la configuration de l'ASA. Dans ce cas, la configuration de l'ASA conserve les commandes d'origine afin que vous puissiez apporter les ajustements nécessaires. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation de l'ASA.

Remarque Vous pouvez modifier les membres d'un EtherChannel alloué sans affecter le périphérique logique.

Avant de commencer

- Configurez vos interfaces et ajoutez tous les EtherChannels en fonction de Configurer une interface physique, à la page 206 et Ajouter un canal EtherChannel (canal de port), à la page 207.
- Si vous souhaitez ajouter une interface déjà allouée à un EtherChannel (par exemple, toutes les interfaces sont allouées par défaut à une grappe), vous devez d'abord désallouer l'interface du périphérique logique, puis ajouter l'interface à l'EtherChannel. Pour un nouvel EtherChannel, vous pouvez ensuite l'affecter au périphérique.
- Si vous souhaitez remplacer l'interface de gestion par un EtherChannel de gestion, vous devez créer l'EtherChannel avec au moins une interface de membre de données non allouée, puis remplacer l'interface de gestion actuelle par l'EtherChannel. Une fois l'ASA rechargé (les modifications de l'interface de gestion entraînent un redémarrage), vous pouvez également ajouter l'interface de gestion (désormais non allouée) à l'EtherChannel.
- Pour la mise en grappe ou le basculement, assurez-vous d'ajouter ou de supprimer l'interface sur toutes les unités. Nous vous recommandons d'effectuer les modifications d'interface d'abord sur l'unité de données ou de secours, puis sur l'unité de contrôle ou l'unité active. Les nouvelles interfaces sont ajoutées dans un état administrativement inactif, de sorte qu'elles n'affectent pas la supervision des interfaces.

Procédure

Étape 1 Dans Firewall Chassis Manager, sélectionner **Logical Devices (dispositifs logiques)**.

Étape 2 Cliquez sur l'icône **Edit** (modifier) en haut à droite pour modifier le périphérique logique.

Étape 3 Annulez l'allocation d'une interface de données en désélectionnant l'interface dans la zone **Data Ports** (Ports de données).

Étape 4 Attribuez une nouvelle interface de données en la sélectionnant dans la zone **Data Ports** (Ports de données).

Étape 5 Remplacez l'interface de gestion :

Pour ce type d'interface, le périphérique se recharge après que vous ayez enregistré vos modifications.

a) Cliquez sur l'icône de périphérique au centre de l'écran.
b) Dans l'onglet **General/Cluster Information** (Général/Renseignements sur la grappe), choisissez la nouvelle **interface de gestion** dans la liste déroulante.
c) Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer).

Se connecter à la console de l'application

Suivez la procédure ci-dessous pour vous connecter à la console de l'application.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

connect module *slot_number* {**console** | **telnet**}

Pour vous connecter au moteur de sécurité d'un périphérique qui ne prend pas en charge plusieurs modules de sécurité, utilisez toujours **1** comme *slot_number*.

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Étape 2 Connectez-vous à la console d'application.

connect asa *name*

Pour afficher les noms des instances, entrez la commande sans nom.

Exemple :

```
Firepower-module1> connect asa asa1
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

Étape 3 Quittez la console d'application pour accéder à l'interface de ligne de commande du module FXOS.

- ASA : Saisissez **Ctrl-a, d**

Étape 4 Revenez au niveau de superviseur de l'Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

Exemple

Dans l'exemple suivant, une connexion est établie à un ASA sur le module de sécurité 1, puis retourne au niveau de superviseur du l'Interface de ligne de commande FXOS.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

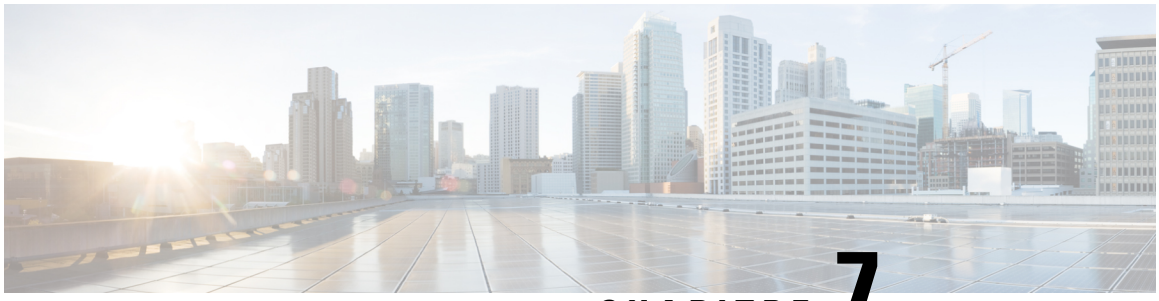
Firepower-module1>connect asa asa1
asa> ~
telnet> quit
Connection closed.
Firepower#
```

Historique des périphériques logiques

Fonctionnalités	Version	Détails
ASA pour le Firepower 4112	9.14(1)	Nous avons lancé le Firepower 4112. **Remarque** FXOS 2.8.1 est nécessaire.
Prise en charge du Firepower 9300 SM-56	9.12.2	Nous avons lancé le module de sécurité SM-56. **Remarque** FXOS 2.6.1.157 est nécessaire.
ASA pour les Firepower 4115, 4125 et 4145	9.12(1)	Nous avons lancé les Firepower 4115, 4125 et 4145. **Remarque** FXOS 2.6.1 est nécessaire.
Prise en charge des Firepower 9300 SM-40 et SM-48	9.12.1	Nous avons lancé les modules de sécurité SM-40 et SM-48. **Remarque** FXOS 2.6.1 est nécessaire.
Prise en charge d'ASA et de Firewall Threat Defense sur des modules distincts du même Firepower 9300	9.12.1	Vous pouvez maintenant déployer ASA et des périphériques logiques Firewall Threat Defense sur le même Firepower 9300. **Remarque** FXOS 2.6.1 est nécessaire.

Fonctionnalités	Version	Détails
Adresse IP personnalisable par liaison de commande de grappe pour le Firepower 4100/9300	9.10.1	Par défaut, la liaison de commande de grappe utilise le réseau 127.2.0.0/16. Vous pouvez maintenant définir le réseau lorsque vous déployez la grappe dans FXOS. Le châssis génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID du châssis et de l'ID d'emplacement : 127.2.*chassis_id*.*slot_id*. Cependant, certains déploiements réseau ne permettent pas le passage du trafic 127.2.0.0/16. Par conséquent, vous pouvez maintenant définir un sous-réseau personnalisé /16 pour la liaison de commande de grappe dans FXOS, à l'exception des adresses de boucle avec retour (127.0.0.0/8) et de multidiffusion (224.0.0.0/4). **Remarque** FXOS 2.4.1 est nécessaire. Écrans nouveaux ou modifiés de Firepower Chassis Manager : **Logical Devices (Périphériques logiques)** > **Add Device (Ajouter un périphérique)** > **Cluster Information (Renseignements relatifs à la grappe)** > champ **CCL Subnet IP** (Adresse IP du sous-réseau CCL)
Prise en charge des données EtherChannels en mode activé	9.10.1	Vous pouvez maintenant définir les données et les EtherChannels de partage de données en mode LACP actif ou en mode Activé. Les autres types d'EtherChannels ne prennent en charge que le mode actif. **Remarque** FXOS 2.4.1 est nécessaire. Écrans du gestionnaire de châssis Firepower nouveaux ou modifiés : **Interfaces** > **All Interfaces(Toutes les interfaces)** > **Edit Port Channel (Modifier le canal de port)** > **Mode**
Amélioration de la mise en grappe inter-sites pour l'ASA sur le Châssis Firepower 4100/9300	9.7(1)	Vous pouvez maintenant configurer l'ID de site pour chaque Châssis Firepower 4100/9300 lorsque vous déployez la grappe ASA. Auparavant, vous deviez configurer l'ID de site dans l'application ASA; cette nouvelle fonctionnalité facilite le déploiement initial. Notez que vous ne pouvez plus définir l'ID de site dans la configuration ASA. En outre, pour une meilleure compatibilité avec la mise en grappe inter-sites, nous vous recommandons de mettre à niveau vers ASA 9.7(1) et FXOS 2.1.1, ce qui comprend plusieurs améliorations de la stabilité et des performances. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)**
Prise en charge de Firepower 4100	9.6(1)	Avec FXOS 1.1.4, l'ASA prend en charge la mise en grappe inter-châssis sur le Firepower 4100. Nous n'avons pas modifié d'écrans.

Fonctionnalités	Version	Détails
Mise en grappe inter-châssis pour 6 modules et mise en grappe inter-sites pour l'application ASA Firepower 9300	9.5(2.1)	Grâce à FXOS 1.1.3, vous pouvez désormais activer la mise en grappe inter-châssis et par extension inter-sites. Vous pouvez inclure jusqu'à 6 modules dans un maximum de 6 châssis. Nous n'avons pas modifié d'écrans.
Mise en grappe d'ASA intra-châssis pour le Firepower 9300	9.4(1.150)	Vous pouvez mettre en grappe jusqu'à 3 modules de sécurité dans le châssis Firepower 9300. Tous les modules dans le châssis doivent appartenir à la grappe. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster Replication (Réplication de grappe ASA)**



CHAPITRE 7

Mode pare-feu transparent ou routé

Ce chapitre décrit comment définir le mode du pare-feu routé ou transparent, ainsi que le fonctionnement du pare-feu dans chaque mode de pare-feu.

Vous pouvez définir le mode de pare-feu indépendamment pour chaque contexte en mode de contexte multiple.

- Mode pare-feu, à la page 219
- Paramètres de défaut, à la page 229
- Lignes directrices sur le mode pare-feu, à la page 229
- Définir le mode du pare-feu (mode unique), à la page 231
- Exemples de mode de pare-feu, à la page 232
- Historique du mode de pare-feu, à la page 243

Mode pare-feu

Un périphérique ASA prend en charge deux modes de pare-feu :

- Mode de pare-feu routé
- Mode de pare-feu transparent

Mode de pare-feu routé

En mode routage, l'ASA est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Vous pouvez partager des interfaces de couche 3 entre les contextes.

Fonctionnalités intégrées de routage et de pontage

Avec le routage et le pont intégrés, vous pouvez utiliser un « groupe de ponts » dans lequel vous regroupez plusieurs interfaces sur un réseau, et l'ASA utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface virtuelle de pont (BVI) à laquelle vous attribuez une adresse IP sur le réseau. Les routes ASA entre les BVI et les interfaces de routage normales. Si vous n'avez pas besoin du mode à contextes multiples ou de mise en grappe, ni d'interfaces membres EtherChannel ou VNI, vous pouvez envisager d'utiliser le mode routé au lieu du mode transparent. En mode routé, vous pouvez avoir un ou plusieurs groupes de ponts isolés comme en mode transparent, mais vous pouvez également avoir des interfaces de routage normales pour un déploiement mixte.

Mode de pare-feu transparent

Classiquement, un pare-feu est un saut routé et agit comme une passerelle par défaut pour les hôtes qui se connectent à l'un de ses sous-réseaux filtrés. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés. Cependant, comme tout autre pare-feu, le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications normales de pare-feu sont en place.

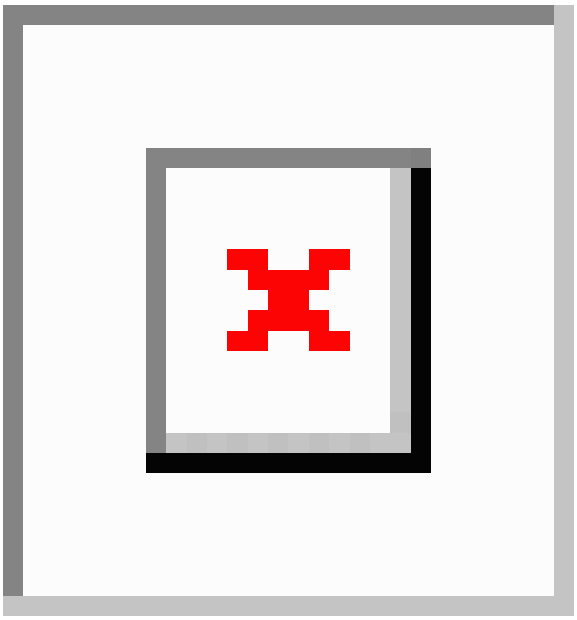
La connectivité de couche 2 est obtenue à l'aide d'un « groupe de ponts » où vous regroupez les interfaces interne et externe d'un réseau, où l'ASA utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface virtuelle de pont (BVI) à laquelle vous attribuez une adresse IP sur le réseau. Vous pouvez avoir plusieurs groupes de ponts pour plusieurs réseaux. En mode transparent, ces groupes de ponts ne peuvent pas communiquer entre eux.

Utilisation d'un réseau de pare-feu transparent

L'ASA relie le même réseau entre ses interfaces. Étant donné que le pare-feu n'est pas un tronçon de routage, vous pouvez facilement introduire un pare-feu transparent dans un réseau existant.

La figure suivante montre un réseau de pare-feu transparent typique où les périphériques externes se trouvent sur le même sous-réseau que les périphériques internes. Le routeur interne et les hôtes semblent être directement connectés au routeur externe.

Illustration 28 : Réseau de pare-feu transparent



Interface Management (gestion)

En plus de chaque adresse IP d'interface virtuelle de pont (BVI), vous pouvez ajouter une interface de Management (gestion) *logement*/*port* distincte qui ne fait partie d'aucun groupe de ponts et qui autorise uniquement le trafic de gestion vers l'ASA. Pour obtenir plus de renseignements, consultez Interface de gestion, à la page 612.

Passage de trafic pour les fonctionnalités en mode routé

Pour les fonctionnalités qui ne sont pas directement prises en charge sur le pare-feu transparent, vous pouvez laisser le trafic passer pour que les routeurs en amont et en aval prennent en charge la fonctionnalité.

Types de trafic pris en charge

Par exemple, en utilisant une règle d'accès, vous pouvez autoriser le trafic DHCP (au lieu de la fonction de relais DHCP non prise en charge) ou le trafic de multidiffusion comme celui créé par IP/TV. Vous pouvez également établir des contiguïtés de protocole de routage par l'intermédiaire d'un pare-feu transparent; vous pouvez autoriser le trafic OSPF, RIP, EIGRP ou BGP en fonction d'une règle d'accès. De même, des protocoles comme HSRP ou VRRP peuvent passer par l'ASA.

Groupes de ponts

Un groupe de ponts est un groupe d'interfaces que ASA relie par des ponts au lieu de routes. Les groupes de ponts sont pris en charge à la fois en mode transparent et en mode pare-feu routé. Comme toute autre interface de pare-feu, le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications normales de pare-feu sont en place.

Interfaces virtuelles de pont

Chaque groupe de ponts comprend une interface virtuelle de pont (BVI). ASA utilise l'adresse IP des BVI comme adresse source pour les paquets provenant du groupe de ponts. L'adresse IP BVI doit se trouver sur le même sous-réseau que les interfaces membres du groupe de ponts. Les BVI ne prennent pas en charge le trafic sur les réseaux secondaires; seul le trafic sur le même réseau que l'adresse IP BVI est pris en charge.

Fonctionnalité BVI par mode

En mode transparent : seules les interfaces des membres du groupe de ponts sont nommées et peuvent être utilisées avec les fonctionnalités basées sur l'interface.

En mode routé : les BVI servent de passerelle entre le groupe de ponts et les autres interfaces routées. Pour le routage entre groupes de ponts/interfaces routées, vous devez nommer le BVI. Pour certaines fonctionnalités basées sur l'interface, vous pouvez utiliser le BVI lui-même :

- Access Rules (règles d'accès) : vous pouvez configurer des règles d'accès pour les interfaces des membres des groupes de ponts et pour les BVI; pour les règles de trafic entrant, l'interface membre est vérifiée en premier. Pour les règles de trafic sortant, les BVI sont vérifiés en premier.
- Serveur DHCPv4 : seuls les BVI prennent en charge la configuration de serveur DHCPv4.
- Routes statiques : vous pouvez configurer des routes statiques pour les BVI; vous ne pouvez pas configurer de routage statique pour les interfaces membres.
- Serveur syslog et autre trafic provenant de l'ASA : lorsque vous spécifiez un serveur syslog (ou un serveur SNMP, ou un autre service où le trafic provient de l'ASA), vous pouvez spécifier une interface BVI ou une interface membre.

Si vous ne nommez pas les BVI en mode routé, ASA n'acheminera pas le trafic du groupe de ponts. Cette configuration reproduit le mode de pare-feu transparent pour le groupe de ponts. Si vous n'avez pas besoin du mode à contextes multiples ni de mise en grappe, ni d'interfaces membre EtherChannel ou VNI, vous pouvez envisager d'utiliser le mode routé à la place. En mode routé, vous pouvez avoir un ou plusieurs groupes

de ponts isolés comme en mode transparent, mais vous pouvez également avoir des interfaces de routage normales pour un déploiement mixte.

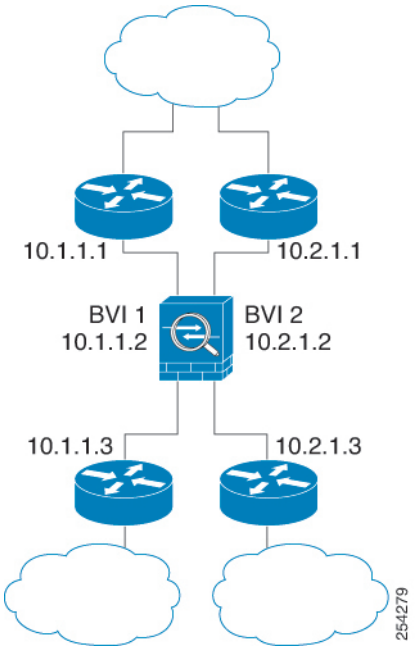
Groupes de ponts en mode pare-feu transparent

Le trafic des groupes de ponts est isolé des autres groupes de ponts; le trafic n'est pas acheminé vers un autre groupe de ponts dans ASA, et le trafic doit quitter ASA avant d'être acheminé par un routeur externe vers un autre groupe de ponts dans ASA. Bien que les fonctions de pont soient distinctes pour chaque groupe de ponts, de nombreuses autres fonctions sont partagées entre tous les groupes de ponts. Par exemple, tous les groupes de ponts partagent une configuration de serveur syslog ou de serveur AAA. Pour une séparation complète des politiques de sécurité, utilisez les contextes de sécurité avec un groupe de ponts dans chaque contexte.

Vous pouvez inclure plusieurs interfaces par groupe de ponts. Consultez Lignes directrices sur le mode pare-feu, à la page 229 pour connaître le nombre exact de groupes de ponts et d'interfaces pris en charge. Si vous utilisez plus de deux interfaces par groupe de ponts, vous pouvez contrôler la communication entre plusieurs segments du même réseau, et pas seulement entre l'intérieur et l'extérieur. Par exemple, s'il y a trois segments internes avec lesquels vous ne souhaitez pas communiquer, vous pouvez placer chaque segment sur une interface distincte et les autoriser uniquement à communiquer avec l'interface externe. Vous pouvez également personnaliser les règles d'accès entre les interfaces pour autoriser uniquement les accès souhaités.

La figure suivante montre deux réseaux connectés à un ASA, qui comporte deux groupes de ponts.

Illustration 29 : Réseau de pare-feu transparent avec deux groupes de ponts



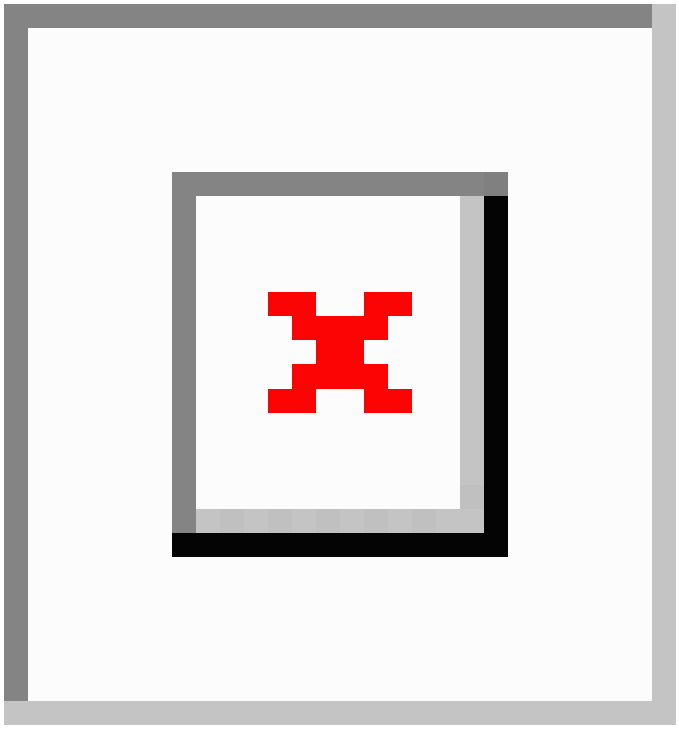
Groupes de ponts en mode pare-feu routé

Le trafic de groupe de ponts peut être acheminé vers d'autres groupes de ponts ou interfaces routées. Vous pouvez choisir d'isoler le trafic de groupe de ponts en n'attribuant pas de nom à l'interface BVI pour le groupe de ponts. Si vous nommez les BVI, alors les BVI participent au routage comme toute autre interface standard.

Utilisation et configuration du groupe de ponts

Une des utilisations d'un groupe de ponts en mode routé est d'utiliser des interfaces supplémentaires sur ASA au lieu d'un commutateur externe. Par exemple, la configuration par défaut de certains périphériques inclut une interface externe en tant qu'interface standard, puis toutes les autres interfaces affectées au groupe de ponts internes. Comme le but de ce groupe de ponts est de remplacer un commutateur externe, vous devez configurer une politique d'accès afin que toutes les interfaces du groupe de ponts puissent communiquer librement. Par exemple, comme dans la configuration par défaut, réglez toutes les interfaces au même niveau de sécurité, puis activez la communication de l'interface de même sécurité; aucune règle d'accès n'est requise.

Illustration 30 : Réseau de pare-feu routé avec un groupe de ponts interne et une interface routée externe



Transmission du trafic non autorisée en mode routé

En mode routé, certains types de trafic ne peuvent pas traverser l'ASA, même si vous l'autorisez dans un critère d'accès. Le groupe de ponts peut toutefois autoriser la quasi-totalité du trafic à passer en utilisant un critère d'accès (pour le trafic IP) ou une règle EtherType (pour le trafic non IP) :

- Trafic IP : en mode de pare-feu routé, le trafic de diffusion et de multidiffusion est bloqué même si vous l'autorisez dans un critère d'accès, y compris les protocoles de routage dynamique non pris en charge et le protocole DHCP (sauf si vous configurez le relais DHCP). Dans un groupe de ponts, vous pouvez autoriser ce trafic avec un critère d'accès.
- Trafic non IP : AppleTalk, IPX, BPDU et MPLS, par exemple, peuvent être configurés pour passer par une règle EtherType.

Remarque Le groupe de ponts ne transmet pas les paquets CDP ni les paquets qui n'ont pas d'EtherType valide supérieur ou égal à 0x600. Une exception est faite pour les BPDU et IS-IS, qui sont pris en charge.

Autorisation du trafic de couche 3

Cette rubrique décrit comment différents types de trafic de couche 3 sont traités par des groupes de ponts et les exigences des règles d'accès pour chaque type de trafic.

- Le trafic IPv4 et IPv6 de monodiffusion est autorisé par le groupe de ponts automatiquement d'une interface à sécurité supérieure vers une interface à sécurité inférieure, sans règle d'accès.
- Pour le trafic de couche 3 passant d'une interface de sécurité faible à une interface de sécurité élevée, une règle d'accès est requise sur l'interface de sécurité faible.
- Les protocoles ARP sont autorisés dans le groupe de ponts dans les deux sens sans règle d'accès. Le trafic ARP peut être contrôlé par inspection ARP.
- Les paquets de découverte de voisin IPv6 et de sollicitation de routeur peuvent être transmis à l'aide de règles d'accès.
- Le trafic en diffusion et en multidiffusion peut être transmis à l'aide de règles d'accès.

Adresses MAC autorisées

Les adresses MAC de destination suivantes sont autorisées par le biais du groupe de ponts si elles le sont par votre politique d'accès (voir Autorisation du trafic de couche 3, à la page 224). Toute adresse MAC qui ne figure pas dans cette liste est abandonnée.

- VRAIE adresse MAC de destination de diffusion égale à FFFF.FFFF.FFFF
- Adresses MAC IPv4 de multidiffusion, de 0100.5E00.0000 à 0100.5EFE.FFFF
- Adresses MAC IPv6 de multidiffusion, de 3333.0000.0000 à 3333.FFFF.FFFF
- Adresse de multidiffusion BPDU égale à 0100.0CCC.CCCD
- Adresses MAC AppleTalk de multidiffusion, de 0900.0700.0000 à 0900.07FF.FFFF

BPDU Handling (gestion des paquets BPDU)

Pour éviter les boucles avec le protocole Spanning Tree, les BPDU (Bridge Protocol Data Unit, Unité de données du protocole de pont) sont transmises par défaut. Pour bloquer les BPDU, vous devez configurer une règle EtherType pour les refuser. Vous pouvez également bloquer les BPDU sur les commutateurs externes. Par exemple, vous pouvez bloquer des BPDU sur le commutateur si des membres du même groupe de ponts sont connectés aux ports de commutation de différents VLAN. Dans ce cas, les BPDU d'un VLAN seront visibles dans l'autre VLAN, ce qui peut causer des problèmes de processus de sélection du pont racine du protocole Spanning Tree.

Si vous utilisez le basculement, vous souhaiterez peut-être bloquer les BPDU pour empêcher le port de commutation de passer à l'état de blocage lorsque la topologie change. Consultez Exigences en matière de groupes de ponts pour le basculement, à la page 305 pour de plus amples renseignements.

Recherches d'adresse MAC ou de route

Pour le trafic à l'intérieur d'un groupe de ponts, l'interface sortante d'un paquet est déterminée en effectuant une recherche d'adresse MAC de destination plutôt qu'une recherche de route.

Cependant, les recherches de routage sont nécessaires dans les situations suivantes :

- Trafic provenant de l'ASA : ajoutez une voie de routage statique/par défaut sur l'ASA pour le trafic destiné à un réseau distant où se trouve un serveur syslog, par exemple.
- Politique SSL activée en mode de pare-feu transparent :
  - Le trafic TLS 1.3 passe par le périphérique ASA.
  - ASA agit en tant que proxy TCP. Il met fin à la connexion TCP du côté client et amorce une connexion distincte du côté du serveur. La pile TCP ASA est propriétaire de l'état de la session.
  - Pour les sessions proxy inactives, ASA génère des sondes Keepalive ACK du protocole TCP pour conserver l'état de la connexion. Il ne s'agit pas de paquets d'intercommunication : le pare-feu les crée et les envoie au client ou au serveur en fonction de l'état de la connexion de transit TLS.
  - Comme l'ASA est à l'origine de ces éléments Keepalives, il doit effectuer une recherche dans la table d'adjacence (résolution MAC de saut suivant ou de sortie) même en mode transparent.
  - Si la recherche d'adjacence échoue pour l'un de ces paquets générés par le proxy, l'ASA consigne le journal système 110003.

    Pour éviter ces messages syslog, configurez les routes sur l'ASA pour les points terminaux de la connexion de transit (adresses IP du client et du serveur). Un routage adéquat permet des recherches d'adjacence réussies pour les paquets Keepalive.

    Si l'ASA envoie un TCP Keepalive et reçoit une réponse, il maintient la connexion de transit active. Si le périphérique ne peut pas envoyer les Keepalives ou ne reçoit aucune réponse, il supprime la connexion de transit après environ 240 secondes.
- Trafic de voix sur IP (VoIP) et TFTP avec inspection activée, et le point terminal se trouve à au moins un saut (ajouter une route statique sur l'ASA pour le trafic destiné au point terminal distant afin que les connexions secondaires soient réussies. L'ASA crée un « trou » temporaire dans la politique de contrôle d'accès pour autoriser la connexion secondaire; et comme la connexion peut utiliser un ensemble d'adresses IP différent de celui de la connexion principale, l'ASA doit effectuer une recherche de routage pour installer le sténopé sur la bonne interface.

  Parmi les autres applications concernées, on trouve :
  - CTIQBE
  - GTP
  - H.323
  - MGCP
  - RTSP
  - SIP et Skinny (SCCP)
  - SQL*Net
  - SunRPC

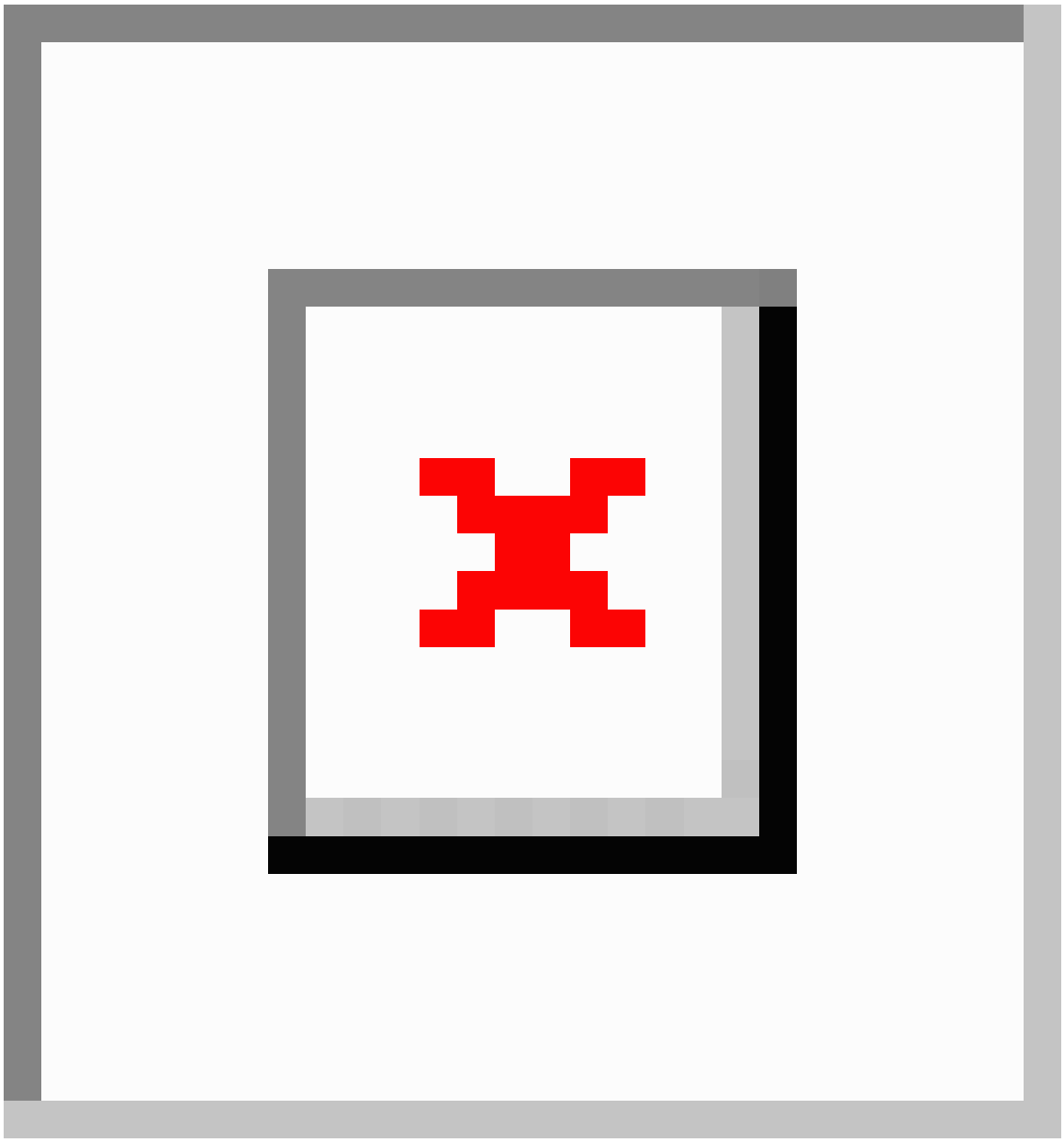
- TFTP

- Trafic à au moins un saut de distance pour lequel l'ASA exécute la NAT - Configurer une route statique sur l'ASA pour le trafic destiné au réseau distant. Vous avez également besoin d'une route statique sur le routeur en amont pour que le trafic destiné aux adresses mappées soit envoyé à l'ASA.

  Cette exigence de routage est également vraie pour les adresses IP intégrées pour VoIP et DNS avec inspection et NAT activées, et les adresses IP intégrées sont à au moins un sautillement. L'ASA doit identifier la bonne interface de sortie pour pouvoir effectuer la traduction.

NAT dans un groupe de pont

Illustration 31 : Exemple de NAT : NAT dans un groupe de pont



Fonctionnalités non prises en charge pour les groupes de ponts en mode transparent

Le tableau suivant répertorie les fonctionnalités non prises en charge dans les groupes de ponts en mode transparent.

Tableau 10 : Fonctionnalités non prises en charge en mode transparent

Fonctionnalités	Description
DNS dynamique	—
Serveur sans état DHCPv6	Seul le serveur DHCPv4 est pris en charge sur les interfaces membres des groupes de ponts.
Relais DHCP	Le pare-feu transparent peut servir de serveur DHCPv4, mais il ne prend pas en charge le relais DHCP. Le relais DHCP n'est pas nécessaire, car vous pouvez permettre au trafic DHCP de passer en utilisant deux règles d'accès : une qui autorise les requêtes DHCP de l'interface interne vers l'extérieur et une qui autorise les réponses du serveur dans l'autre sens.
Protocoles de routage dynamique	Vous pouvez, cependant, ajouter des routes statiques pour le trafic provenant des interfaces ASA pour les membres des groupes de ponts. Vous pouvez également autoriser les protocoles de routage dynamique à l'aide de l'ASA en utilisant une règle d'accès.
Routage de multidiffusion IP	Vous pouvez autoriser le trafic en multidiffusion via l'ASA en l'autorisant dans une règle d'accès.
Qualité de service	—
Terminaison VPN pour le trafic traversant	Le pare-feu transparent prend en charge les tunnels VPN de site à site pour les connexions de gestion uniquement sur les interfaces membres des groupes de ponts. Il ne met pas fin aux connexions VPN pour le trafic passant par ASA. Vous pouvez faire passer le trafic VPN par l'ASA à l'aide d'un critère d'accès, mais cela ne met pas fin aux connexions hors gestion.
Communications unifiées	—

Fonctionnalités non prises en charge pour les groupes de ponts en mode routé

Le tableau suivant répertorie les fonctionnalités non prises en charge dans les groupes de ponts en mode routé.

Tableau 11 : Fonctionnalités non prises en charge en mode routé

Fonctionnalités	Description
Interfaces membre EtherChannel ou VNI	Seules les interfaces physiques et les sous-interfaces sont prises en charge en tant qu'interfaces de membres de groupes de ponts. Les interfaces Management (gestion) ne sont pas non plus prises en charge.
Mise en grappe	Les groupes de ponts ne sont pas pris en charge dans la mise en grappe.
DNS dynamique	—
Serveur sans état DHCPv6	Seul le serveur DHCPv4 est pris en charge sur les BVI.

Fonctionnalités	Description
Relais DHCP	Le pare-feu routé peut servir de serveur DHCPv4, mais il ne prend pas en charge le relais DHCP sur les BVI ou les interfaces membres de groupes de ponts.
Protocoles de routage dynamique	Vous pouvez, cependant, ajouter des routes statiques pour les BVI. Vous pouvez également autoriser les protocoles de routage dynamique à l'aide de l'ASA en utilisant une règle d'accès. Les interfaces de groupe sans pont prennent en charge le routage dynamique.
Routage de multidiffusion IP	Vous pouvez autoriser le trafic en multidiffusion via l'ASA en l'autorisant dans une règle d'accès. Les interfaces de groupe sans pont prennent en charge le routage de multidiffusion.
Mode contexte multiple	Les groupes de ponts ne sont pas pris en charge en mode contexte multiple.
Qualité de service	Les interfaces sans groupe de ponts prennent en charge la QoS.
Terminaison VPN pour le trafic traversant	Vous ne pouvez pas mettre fin à une connexion VPN sur les BVI. Les interfaces qui ne font pas partie d'un groupe de pont prennent en charge le VPN. Les interfaces membres des groupes de ponts prennent en charge les tunnels VPN de site à site pour les connexions de gestion uniquement. Il ne met pas fin aux connexions VPN pour le trafic passant par ASA. Vous pouvez faire passer le trafic VPN par le groupe de ponts à l'aide d'une règle d'accès, mais cela ne met pas fin aux connexions hors gestion. Le VPN SSL sans client n'est pas non plus pris en charge.
Communications unifiées	Les interfaces de groupe hors pont prennent en charge les communications unifiées.

Paramètres de défaut

Répertorie les paramètres par défaut pour le mode de pare-feu.

Mode par défaut

Le mode par défaut est le mode routé.

Valeurs par défaut des groupes de ponts

Par défaut, tous les paquets ARP sont transmis au sein du groupe de ponts.

Lignes directrices sur le mode pare-feu

Passez en revue ces lignes directrices relatives au mode de pare-feu.

Lignes directrices relatives au mode contextuel

Définissez le mode de pare-feu par contexte.

Limites de groupe de ponts et exigences de réseau

- Chaque réseau connecté directement doit se trouver sur le même sous-réseau.
- Le périphérique de pare-feu Threat Defense ne prend pas en charge le trafic sur les réseaux secondaires ; seul le trafic sur le même réseau que l'adresse IP BVI est pris en charge.

Exigences relatives à l'adresse IP BVI

- Une adresse IP pour le BVI est requise pour chaque groupe de ponts pour le trafic de gestion vers le périphérique et en provenance du périphérique, ainsi que pour le trafic de données qui doit passer par le périphérique de pare-feu Threat Defense. Pour le trafic IPv4, spécifiez une adresse IPv4. Pour le trafic IPv6, spécifiez une adresse IPv6.
- Vous ne pouvez configurer les adresses IPv6 que manuellement.
- L'adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Vous ne pouvez pas définir le sous-réseau comme sous-réseau d'hôte (255.255.255.255).

Membres du groupe de ponts non pris en charge

- Les interfaces de gestion ne sont pas prises en charge en tant que membres de groupes de ponts.
- Pour l'ASAv50 sur VMware avec des interfaces ixgbevf pontées, le mode transparent n'est pas pris en charge et les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour Série Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour le 200/ 1010/ , il n'est pas possible de mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques au sein du même groupe de ponts.

Exigences et limites du mode transparent

- En mode transparent, vous devez utiliser au moins un groupe de ponts; les interfaces de données doivent appartenir à un groupe de ponts.
- En mode transparent, ne spécifiez pas l'adresse IP des BVI comme passerelle par défaut pour les périphériques connectés; Les périphériques doivent spécifier le routeur de l'autre côté de la ASA comme passerelle par défaut.
- En mode transparent, la voie de routage par défaut, qui est requise pour fournir un chemin de retour au trafic de gestion, n'est appliquée qu'au trafic de gestion provenant d'un réseau de groupe de ponts. En effet, la voie de routage par défaut spécifie une interface dans le groupe de ponts ainsi que l'adresse IP du routeur sur le réseau du groupe de ponts, et vous ne pouvez définir qu'une seule voie de routage par défaut. Si votre trafic de gestion provient de plus d'un réseau de groupes de ponts, vous devez spécifier une voie de routage statique régulière qui identifie le réseau à partir duquel vous attendez le trafic de gestion.
- Le protocole PPPoE n'est pas pris en charge sur l'interface Management (gestion).

Exigences et limites du mode routé

- En mode routé, pour le routage entre les groupes de ponts et les autres interfaces routées, vous devez nommer les BVI.
- En mode routé, les interfaces EtherChannel définies par ASA et VNI ne sont pas prises en charge en tant que membres de groupes de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.

Limitation relative au traitement du trafic

- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de l'ASA lors de l'utilisation de membres de groupe de ponts. S'il y a deux voisins de chaque côté de l'ASA exécutant BFD, alors l'ASA abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.

Définir le mode du pare-feu (mode unique)

Cette section décrit comment changer de mode de pare-feu à l'aide de la CLI. Pour le mode unique et pour le contexte actuellement connecté en mode multiple (généralement le contexte d'administration), vous ne pouvez pas modifier le mode dans ASDM. Pour les autres contextes de modes multiples, vous pouvez définir le mode dans ASDM pour chaque contexte; voir Configurer un contexte de sécurité, à la page 276.



Remarque Nous vous recommandons de définir le mode de pare-feu avant d'effectuer toute autre configuration, car la modification de ce dernier efface la configuration en cours.

Avant de commencer

Lorsque vous changez de mode, l'ASA efface la configuration en cours (voir Lignes directrices sur le mode pare-feu, à la page 229 pour plus d'informations).

- Si vous avez déjà une configuration remplie, assurez-vous de sauvegarder votre configuration avant de modifier le mode. vous pouvez utiliser cette sauvegarde comme référence lors de la création de votre nouvelle configuration.
- Utilisez l'interface de ligne de commande du port de console pour changer de mode. Si vous utilisez tout autre type de session, y compris l'outil de l'interface de ligne de commande ASDM ou SSH, vous serez déconnecté lorsque la configuration sera effacée et vous devrez vous reconnecter à l'ASA en utilisant le port de console dans tous les cas.
- Définissez le mode dans le contexte.



Remarque Pour définir le mode de pare-feu à transparent et également configurer l'accès de gestion ASDM après avoir effacé la configuration, consultez Configurer l'accès ASDM, à la page 25.

Procédure

Définissez le mode de pare-feu sur transparent :

Pare-feu transparent

Exemple :

```
ciscoasa(config)# firewall transparent
```

Pour changer le mode à routé, saisissez la commande **no firewall transparent** (pas de pare-feu transparent).

Remarque Vous n'êtes pas invité à confirmer le changement de mode de pare-feu; la modification se produit immédiatement.

Exemples de mode de pare-feu

Cette section comprend des exemples illustrant la manière dont le trafic circule à travers l'ASA en mode de pare-feu routé et transparent.

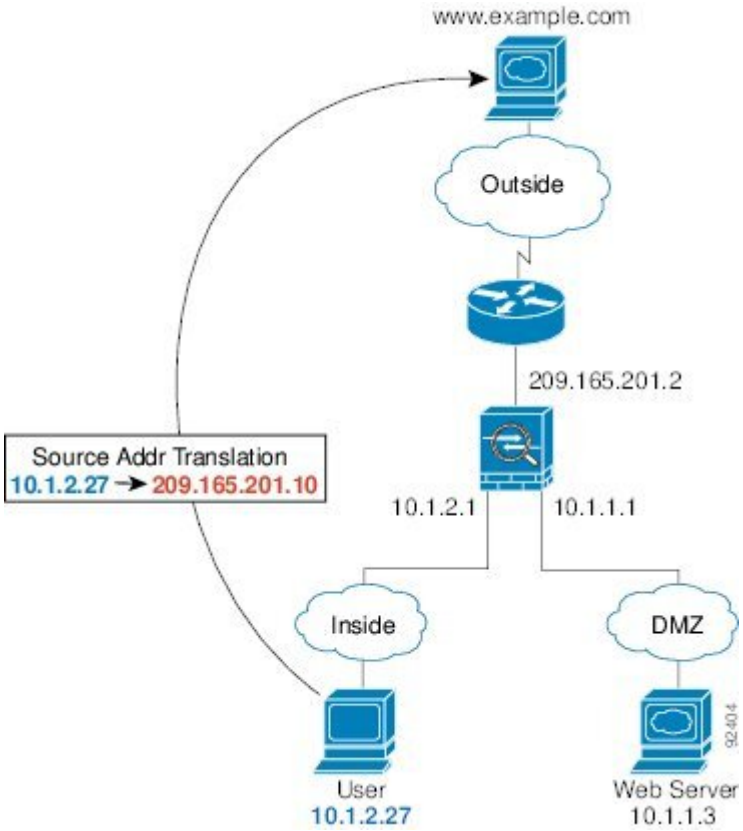
Progression des données dans l'ASA en mode de pare-feu routé

Les sections suivantes décrivent comment les données passent par l'ASA en mode de pare-feu routé dans plusieurs scénarios.

Un utilisateur interne visite un serveur web

La figure suivante montre un utilisateur interne accédant à un serveur web externe.

Illustration 32 : De l'intérieur vers l'extérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. L'utilisateur sur le réseau interne demande une page Web à www.exemple.com.
2. L'ASA reçoit le paquet et, comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

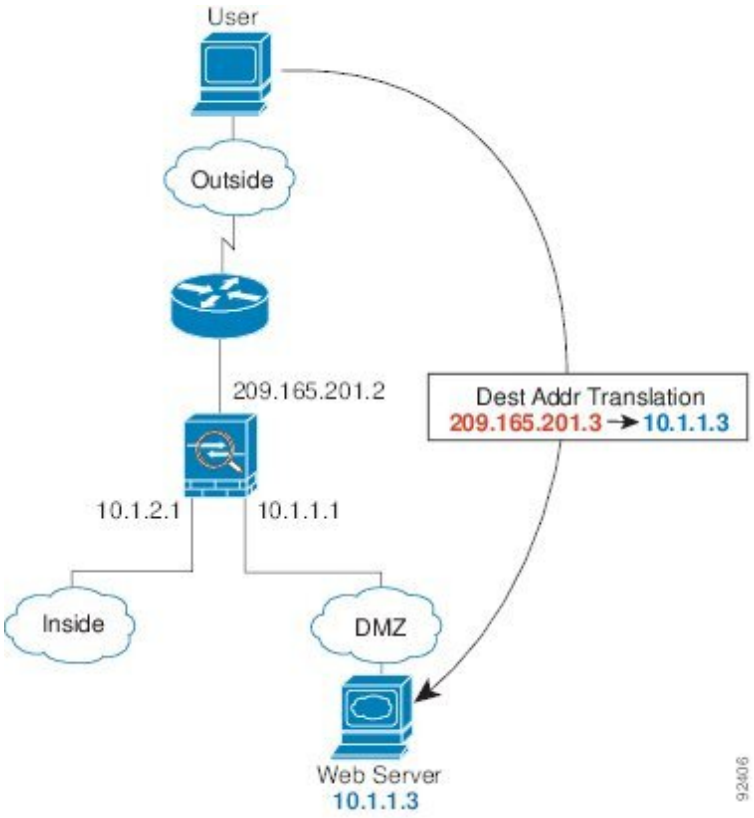
   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. L'ASA traduit l'adresse réelle (10.1.2.27) en adresse mappée 209.165.201.10, qui se trouve sur le sous-réseau de l'interface externe.

   L'adresse mappée peut se trouver sur n'importe quel sous-réseau, mais le routage est simplifié lorsqu'elle se trouve sur le sous-réseau d'interface externe.
4. L'ASA enregistre ensuite qu'une session est établie et transfère le paquet de l'interface externe.
5. Lorsque www.exemple.com répond à la demande, le paquet passe par l'ASA, et comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion. L'ASA effectue la NAT en ne traduisant pas l'adresse de destination globale en adresse d'utilisateur locale, 10.1.2.27.
6. L'ASA transmet le paquet à l'utilisateur interne.

Un utilisateur externe visite un serveur web sur la DMZ

La figure suivante montre un utilisateur externe accédant au serveur web DMZ.

Illustration 33 : Externe vers DMZ



Les étapes suivantes décrivent comment les données passent par l'ASA :

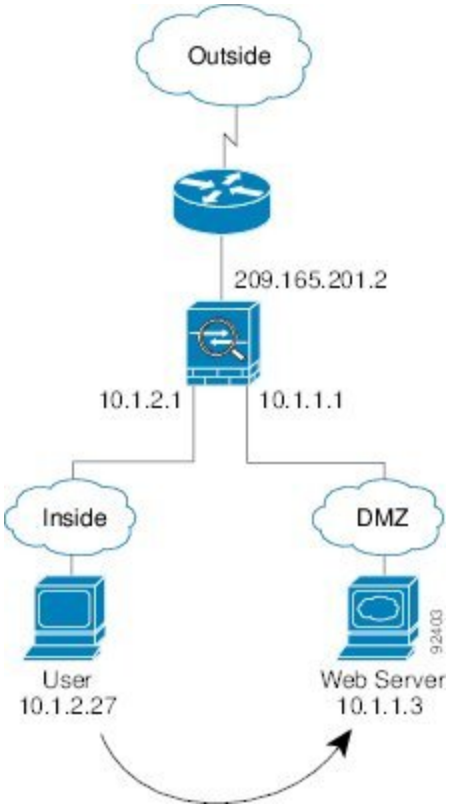
1. Un utilisateur sur le réseau externe demande une page Web au serveur web DMZ en utilisant l'adresse mappée 209.165.201.3, qui se trouve sur le sous-réseau de l'interface externe.
2. L'ASA reçoit le paquet et traduit l'adresse mappée en adresse réelle 10.1.1.3.
3. Comme il s'agit d'une nouvelle session, l'ASA vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
4. L'ASA ajoute ensuite une entrée de session au chemin rapide et transfère le paquet de l'interface DMZ.
5. Lorsque le serveur web DMZ répond à la demande, le paquet passe par l'ASA et, comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion. L'ASA effectue la NAT en traduisant l'adresse réelle en 209.165.201.3.
6. L'ASA transmet le paquet à l'utilisateur externe.

Un utilisateur interne visite un serveur web sur la DMZ

La figure suivante montre un utilisateur interne accédant au serveur web DMZ.

Illustration 34 : Interne à DMZ



Les étapes suivantes décrivent comment les données passent par l'ASA :

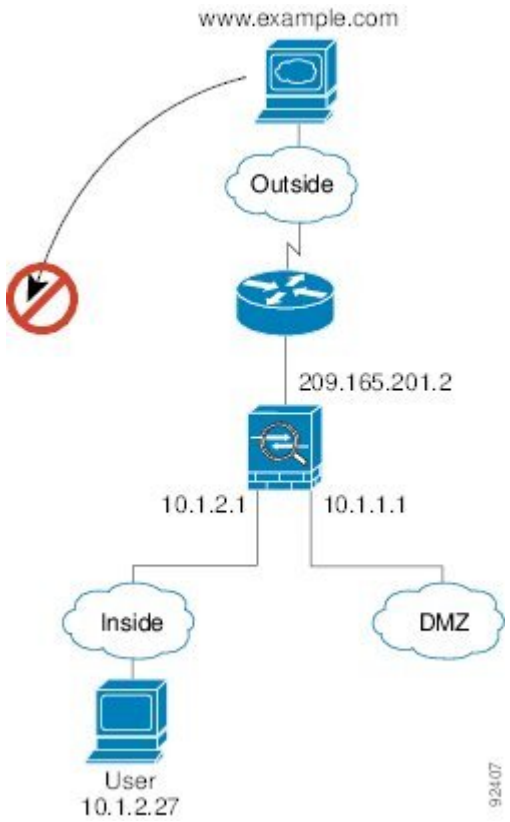
1. Un utilisateur sur le réseau interne demande une page Web au serveur web DMZ en utilisant l'adresse de destination 10.1.1.3.
2. L'ASA reçoit le paquet et, comme il s'agit d'une nouvelle session, l'ASA vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. L'ASA enregistre ensuite qu'une session est établie et transfère le paquet de l'interface DMZ.
4. Lorsque le serveur web DMZ répond à la demande, le paquet emprunte le chemin d'accès rapide, ce qui lui permet de contourner les nombreuses recherches associées à une nouvelle connexion.
5. L'ASA transmet le paquet à l'utilisateur interne.

Un utilisateur externe tente d'accéder à un hôte interne

La figure suivante montre un utilisateur externe qui tente d'accéder au réseau interne.

Illustration 35 : De l'extérieur vers l'intérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. Un utilisateur sur le réseau externe tente d'atteindre un hôte interne (en supposant que l'hôte a une adresse IP routable).

   Si le réseau interne utilise des adresses privées, aucun utilisateur externe ne peut atteindre le réseau interne sans la NAT. L'utilisateur externe peut tenter de joindre un utilisateur interne en utilisant une session NAT existante.

2. L'ASA reçoit le paquet et, parce qu'il s'agit d'une nouvelle session, il vérifie si le paquet est autorisé conformément à la politique de sécurité.

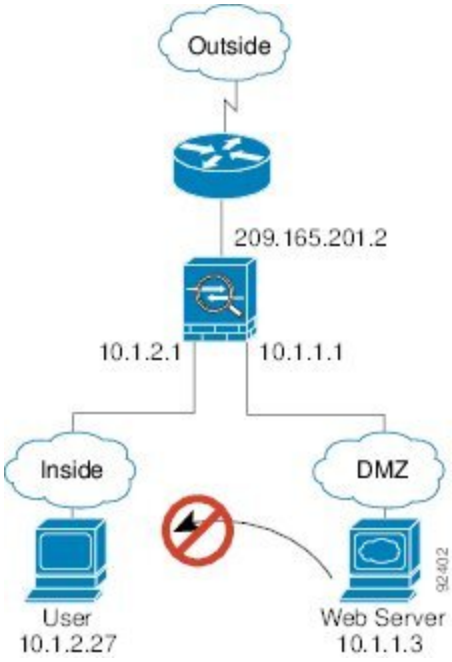
3. Le paquet est refusé et l'ASA abandonne le paquet et consigne la tentative de connexion.

   Si l'utilisateur externe tente d'attaquer le réseau interne, l'ASA utilise de nombreuses technologies pour déterminer si un paquet est valide pour une session déjà établie.

Un utilisateur DMZ tente d'accéder à un hôte interne

La figure suivante montre un utilisateur dans la DMZ tente d'accéder au réseau interne.

Illustration 36 : DMZ vers interne



Les étapes suivantes décrivent comment les données passent par l'ASA :

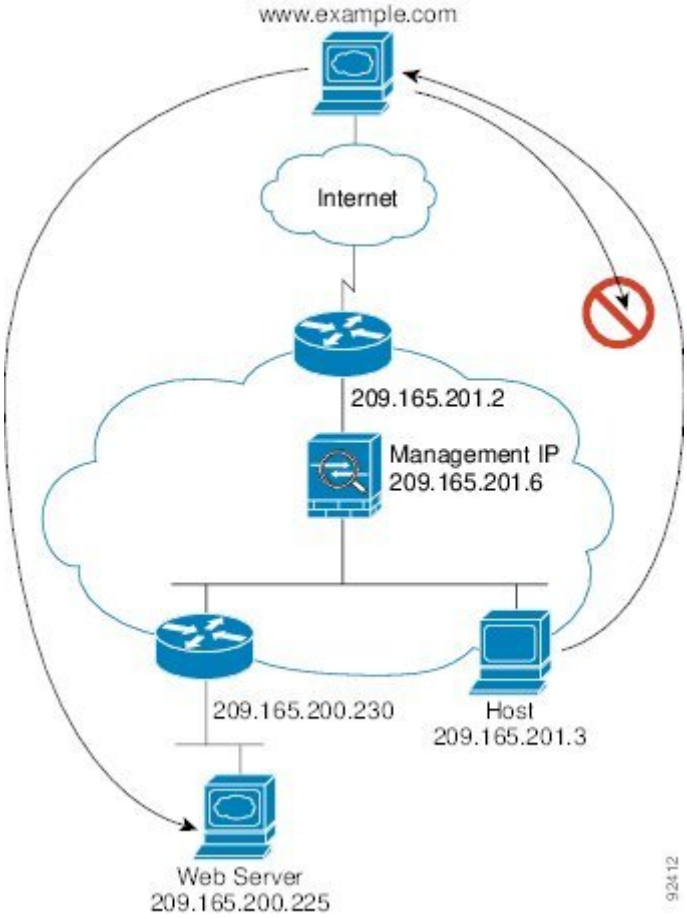
1. Un utilisateur sur le réseau DMZ tente d'atteindre un hôte interne. Étant donné que la DMZ n'a pas à acheminer le trafic sur Internet, le système d'adressage privé n'empêche pas le routage.
2. L'ASA reçoit le paquet et, parce qu'il s'agit d'une nouvelle session, il vérifie si le paquet est autorisé conformément à la politique de sécurité.

   Le paquet est refusé et l'ASA abandonne le paquet et consigne la tentative de connexion.

Progression des données dans le pare-feu transparent

La figure suivante montre une implémentation type de pare-feu transparent avec un réseau interne contenant un serveur Web public. L'ASA comporte un critère d'accès afin que les utilisateurs internes puissent accéder aux ressources Internet. Un autre critère d'accès permet aux utilisateurs externes d'accéder uniquement au serveur Web sur le réseau interne.

Illustration 37 : Chemin de données type d'un pare-feu transparent

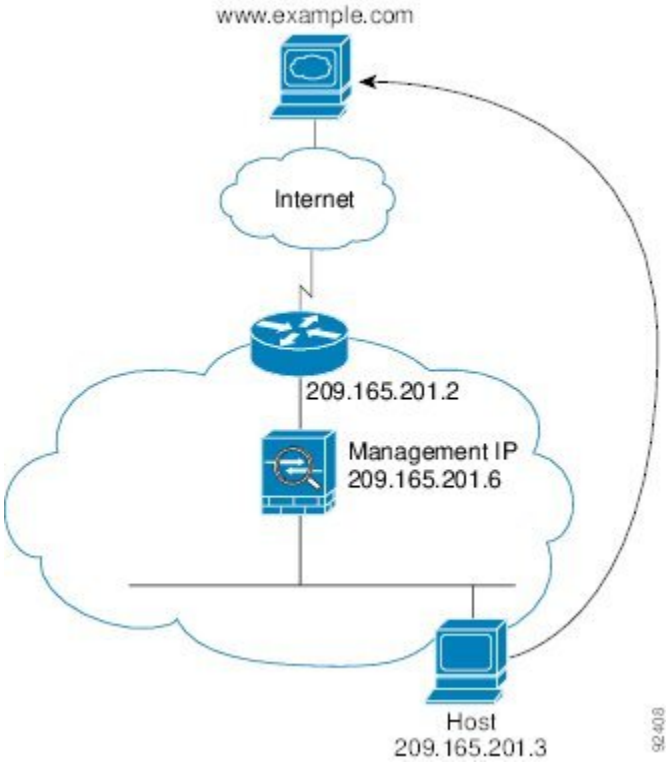


Les sections suivantes décrivent comment les données passent par l'ASA.

Un utilisateur interne visite un serveur web

La figure suivante montre un utilisateur interne accédant à un serveur web externe.

Illustration 38 : De l'intérieur vers l'extérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. L'utilisateur sur le réseau interne demande une page Web à www.exemple.com.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

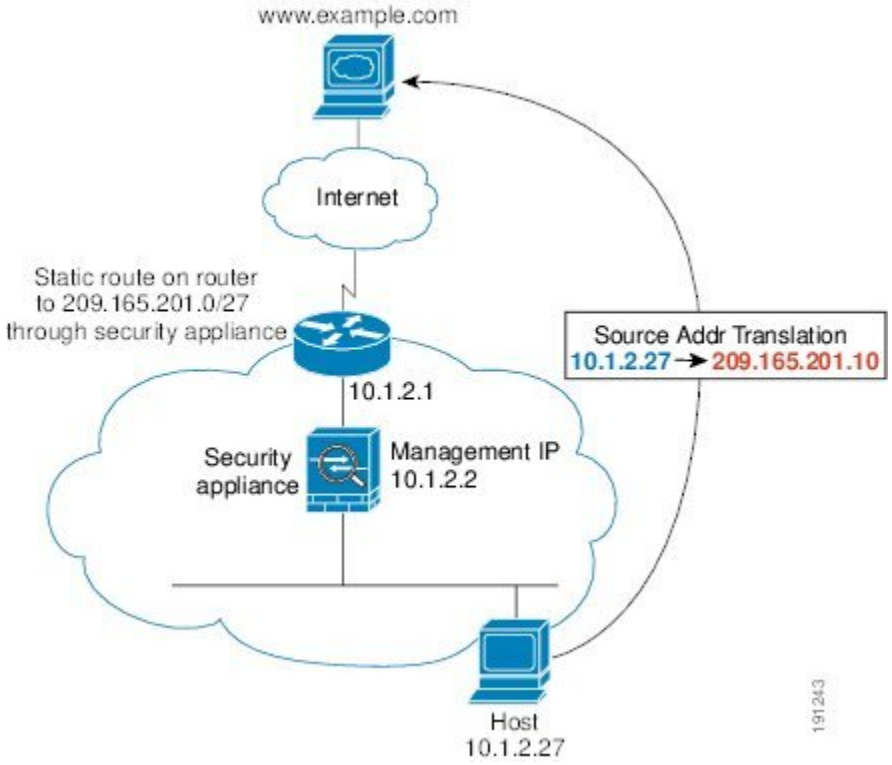
   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. L'ASA enregistre qu'une session est établie.
4. Si l'adresse MAC de destination se trouve dans son tableau, l'ASA transfère le paquet hors de l'interface externe. L'adresse MAC de destination est celle du routeur en amont, 209.165.201.2.

   Si l'adresse MAC de destination ne se trouve pas dans le tableau ASA, il tente de découvrir l'adresse MAC en envoyant une requête ARP ou un message Ping. Le premier paquet est abandonné.
5. Le serveur web répond à la demande; comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion.
6. L'ASA transmet le paquet à l'utilisateur interne.

Un utilisateur interne visite un serveur web à l'aide de la NAT

La figure suivante montre un utilisateur interne accédant à un serveur web externe.

Illustration 39 : De l'intérieur à l'extérieur avec la NAT



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. L'utilisateur sur le réseau interne demande une page Web à www.exemple.com.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet selon une interface unique.
3. L'ASA traduit l'adresse réelle (10.1.2.27) en adresse mappée 209.165.201.10.

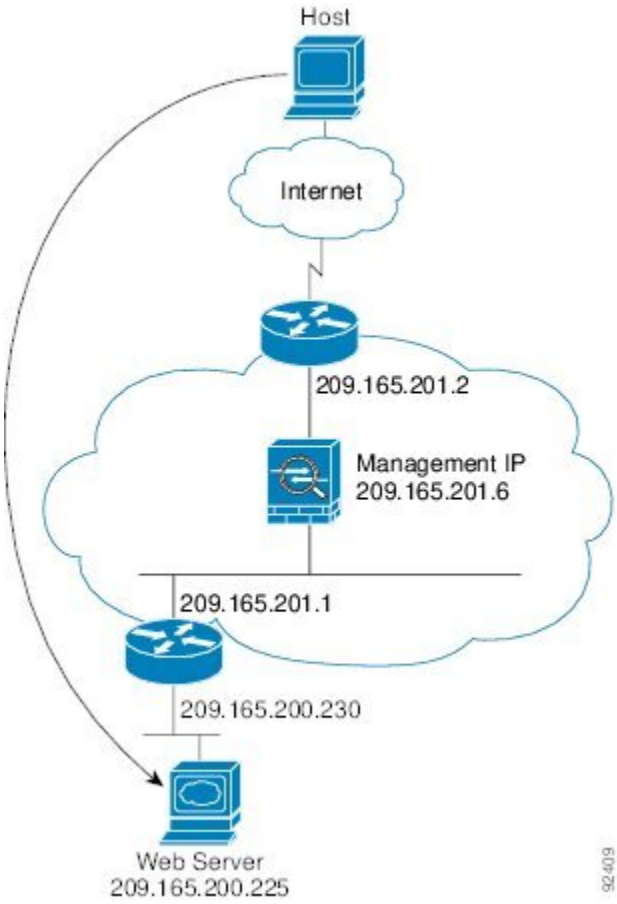
   Étant donné que l'adresse mappée ne se trouve pas sur le même réseau que l'interface externe, assurez-vous que le routeur en amont a une route statique vers le réseau mappé qui pointe vers l'ASA.
4. L'ASA enregistre ensuite qu'une session est établie et transfère le paquet de l'interface externe.
5. Si l'adresse MAC de destination se trouve dans son tableau, l'ASA transfère le paquet hors de l'interface externe. L'adresse MAC de destination est celle du routeur en amont, 10.1.2.1.

   Si l'adresse MAC de destination ne se trouve pas dans le tableau ASA, il tente alors de découvrir l'adresse MAC en envoyant une requête ARP et un message Ping. Le premier paquet est abandonné.
6. Le serveur web répond à la demande; comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion.
7. L'ASA effectue la NAT en ne traduisant pas l'adresse mappée en adresse réelle, 10.1.2.27.

Un utilisateur externe visite un serveur web sur le réseau interne

La figure suivante montre un utilisateur externe accédant au serveur web interne.

Illustration 40 : De l'extérieur vers l'intérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. Un utilisateur sur le réseau externe demande une page Web au serveur web interne.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. L'ASA enregistre qu'une session est établie.
4. Si l'adresse MAC de destination se trouve dans son tableau, l'ASA transfère le paquet hors de l'interface interne. L'adresse MAC de destination est celle du routeur en aval, 209.165.201.1.

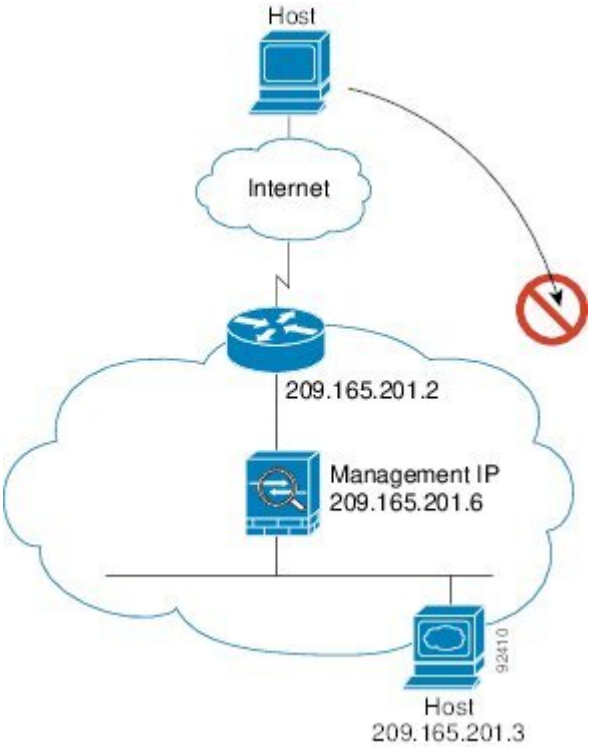
   Si l'adresse MAC de destination ne se trouve pas dans le tableau ASA, il tente alors de découvrir l'adresse MAC en envoyant une requête ARP et un message Ping. Le premier paquet est abandonné.
5. Le serveur web répond à la demande; comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion.

6. L'ASA transmet le paquet à l'utilisateur externe.

Un utilisateur externe tente d'accéder à un hôte interne

La figure suivante montre un utilisateur externe qui tente d'accéder à un hôte sur le réseau interne.

Illustration 41 : De l'extérieur vers l'intérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. Un utilisateur sur le réseau externe tente d'atteindre un hôte interne.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. Le paquet est refusé, car aucun critère d'accès n'autorise l'hôte externe, et l'ASA abandonne le paquet.
4. Si l'utilisateur externe tente d'attaquer le réseau interne, l'ASA utilise de nombreuses technologies pour déterminer si un paquet est valide pour une session déjà établie.

Historique du mode de pare-feu

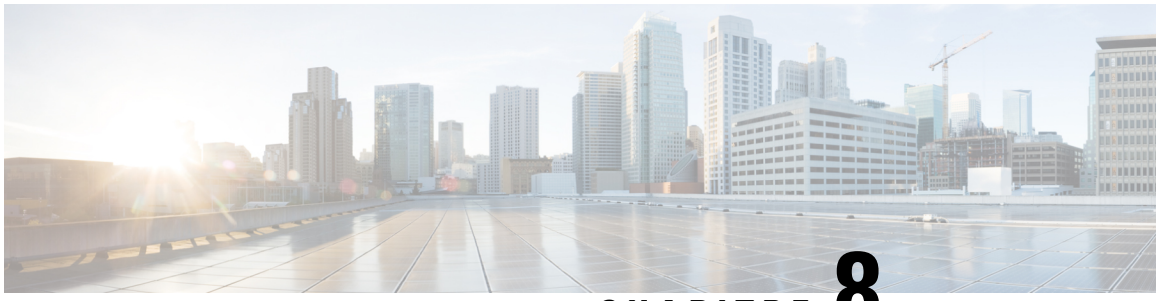
Tableau 12 : Historique des fonctionnalités du mode de pare-feu

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Mode de pare-feu transparent	7.0(1)	Un pare-feu transparent est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés. Nous avons introduit les commandes suivantes : **firewall transparent**, **show firewall**. Vous ne pouvez pas définir le mode de pare-feu dans ASDM; vous devez utiliser l'interface de ligne de commande.
Groupes de ponts de pare-feu transparents	v 8.4(1)	Si vous ne souhaitez pas le surdébit des contextes de sécurité ou si vous souhaitez optimiser votre utilisation des contextes de sécurité, vous pouvez regrouper les interfaces dans un groupe de ponts, puis configurer plusieurs groupes de ponts, un pour chaque réseau. Le trafic de groupe de ponts est isolé des autres groupes de ponts. Vous pouvez configurer jusqu'à 8 groupes de ponts en mode unique ou par contexte en mode multiple, avec 4 interfaces au maximum par groupe de ponts. **Remarque** Bien que vous puissiez configurer plusieurs groupes de ponts sur l'ASA 5505, la restriction de 2 interfaces de données en mode transparent sur l'ASA 5505 signifie que vous ne pouvez utiliser efficacement qu'un seul groupe de ponts. Nous avons modifié ou introduit les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces Configuration (Configuration des interfaces) > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Bridge Group Interface (Ajouter/modifier l'interface de groupe de ponts) Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier l'interface)

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge du mode de pare-feu mixte en mode de contexte multiple	8.5(1)/9.0(1)	Vous pouvez définir le mode de pare-feu indépendamment pour chaque contexte de sécurité en mode de contexte multiple, de sorte que certains puissent s'exécuter en mode transparent et que d'autres s'exécutent en mode routé. Nous avons modifié la commande suivante : **firewall transparent**. Pour le mode unique, vous ne pouvez pas définir le mode de pare-feu dans ASDM; vous devez utiliser l'interface de ligne de commande. Pour le mode multiple, nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité).
Nombre maximum de groupes de ponts en mode transparent augmenté à 250	9.3(1)	Le nombre maximum de groupes de ponts est passé de 8 à 250 groupes de ponts. Vous pouvez configurer jusqu'à 250 groupes de ponts en mode unique ou par contexte en mode multiple, avec 4 interfaces maximum par groupe de ponts. Nous avons modifié les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces Configuration (Configuration des interfaces) > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Bridge Group Interface (Ajouter/modifier l'interface de groupe de ponts) Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier l'interface)
Nombre maximum d'interfaces en mode transparent par groupe de ponts augmenté à 64	9.6(2)	Le nombre maximum d'interfaces par groupe de ponts est passé de 4 à 64. Nous n'avons pas modifié d'écrans.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage et pont intégrés	9.7(1)	Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que l'ASA relie par des ponts au lieu de routes. L'ASA n'est pas un vrai pont, car l'ASA continue d'agir comme un pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place. Auparavant, vous ne pouviez configurer les groupes de ponts qu'en mode de pare-feu transparent, où vous ne pouvez pas effectuer d'acheminement entre les groupes de ponts. Cette fonctionnalité vous permet de configurer des groupes de ponts en mode de pare-feu routé et pour effectuer le routage entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une solution de rechange au commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur l'ASA à affecter au groupe de ponts. En mode routé, les BVI peuvent être une interface nommée et participer séparément des interfaces membres à certaines fonctionnalités, telles que les règles d'accès et le serveur DHCP. Les fonctionnalités suivantes, prises en charge en mode transparent, ne sont pas prises en charge en mode routé : mode de contexte multiple, mise en grappe d'ASA. Les fonctionnalités suivantes ne sont pas prises en charge sur les BVI : le routage dynamique et le routage de multidiffusion. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Static Routes (Routes statiques)** **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Server (Serveur DHCP)** **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Critères d'accès)** **Configuration** > **Firewall (Pare-feu)** > **EtherType Rules (Règles EtherType)**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge du déploiement en mode transparent pour un dispositif logique Firepower 4100/9300 ASA	9.10(1)	Vous pouvez désormais spécifier le mode transparent ou routé lorsque vous déployez l'ASA sur un Firepower 4100/9300 Écrans nouveaux ou modifiés de Firepower Chassis Manager : **Logical Devices (Dispositifs logiques)** > **Add Device (Ajouter un périphérique)** > **Settings (Paramètres)** Options nouvelles ou modifiées : liste déroulante **Firewall Mode**



CHAPITRE 8

Assistant de démarrage

Ce chapitre décrit l'assistant de démarrage ASDM, qui vous guide dans la configuration initiale de l'ASA et vous aide à définir les paramètres de base.

- Accès à l'assistant de démarrage, à la page 247
- Lignes directrices relatives à l'assistant de démarrage, à la page 247
- Écrans de l'assistant de démarrage, à la page 247
- Historique de l'assistant de démarrage, à la page 250

Accès à l'assistant de démarrage

Pour accéder à l'assistant de démarrage, choisissez l'une des options suivantes :

- **Wizards (Assistants) > Startup Wizard (Assistant de démarrage)**.
- **Configuration > Device Setup (Configuration du périphérique) > Startup Wizard (Assistant de démarrage)**, puis cliquez sur **Launch Startup Wizard** (Lancer l'assistant de démarrage).

Lignes directrices relatives à l'assistant de démarrage

Directives relatives au mode contextuel

L'assistant de démarrage n'est pas pris en charge dans le contexte du système.

Écrans de l'assistant de démarrage

La séquence réelle des écrans est déterminée par les sélections de configuration que vous avez spécifiées. Chaque écran est disponible pour tous les modes ou modèles, sauf indication contraire.

Point de départ ou accueil

- Cliquez sur le bouton radio **Modify existing configuration** (Modifier la configuration existante) pour modifier la configuration existante.

- Cliquez sur le bouton radio **Reset configuration to factory defaults** (Réinitialiser la configuration aux valeurs d'usine par défaut) pour définir la configuration aux valeurs d'usine par défaut.
  - Cochez la case **Configure the IP address of the management interface** (Configurer l'adresse IP de l'interface de gestion) pour configurer l'adresse IP et le masque de sous-réseau de l'interface de gestion 0/0 pour qu'ils soient différents de la valeur par défaut (192.168.1.1).



Remarque Si vous réinitialisez la configuration aux valeurs d'usine par défaut, vous ne pouvez pas annuler ces modifications en cliquant sur **Cancel (Annuler)** ou en fermant cet écran.

En mode contexte multiple, cet écran n'inclut aucun paramètre.

Configuration de base

Définissez le nom de domaine, le nom de domaine et activez le mot de passe dans cet écran.

Écrans d'interface

Les écrans d'interface dépendent du mode et du modèle sélectionnés.

Configuration de l'interface externe (mode routé)

- Configurez l'adresse IP de l'interface externe (l'interface avec le niveau de sécurité le plus bas).
- Configurer l'adresse IPv6

Configuration de l'interface externe – PPPoE (mode routé, mode unique)

Configurez les paramètres PPPoE pour l'interface externe.

Configuration de l'adresse IP de gestion (mode transparent)

Pour IPv4, une adresse IP de gestion est requise pour chaque groupe de ponts pour le trafic de gestion et pour que le trafic passe par l'ASA. Cet écran définit l'adresse IP de BVI 1.

Configuration des interfaces

Configurez les paramètres des autres interfaces.

Routes statiques

Configurez les voies de routage statiques.

Serveur DHCP

Configuration du serveur DHCP

Traduction d'adresses réseau (NAT/PAT)

Configure la NAT ou la PAT pour les adresses internes (l'interface avec le niveau de sécurité le plus élevé) lors de l'accès à l'extérieur (l'interface avec le niveau de sécurité le plus bas). Consultez le guide de configuration du pare-feu pour de plus amples renseignements.

Accès administratif

- Configurez l'accès ASDM, Telnet ou SSH.
- Cochez la case **Enable HTTP server for HTTPS/ASDM access** (Activer le serveur HTTP pour l'accès HTTPS/ASDM) pour activer une connexion sécurisée à un serveur HTTP permettant d'accéder à ASDM.
- Cochez la case **Enable ASDM history metrics** (Activer les mesures d'historique ASDM).

Configuration de base de l'IPS

En mode contexte unique, utilisez l'assistant de démarrage dans ASDM pour configurer la configuration de base du réseau IPS. Ces paramètres sont enregistrés dans la configuration IPS, et non dans la configuration ASA. Pour en savoir plus, reportez-vous au guide de démarrage rapide de l'IPS.

Configuration de base ASA CX (ASA 5585-X)

Vous pouvez utiliser Startup Wizard (Assistant de démarrage) dans ASDM pour configurer l'adresse de gestion ASA CX et Auth Proxy Port (Port du proxy d'authentification). Ces paramètres sont enregistrés dans la configuration ASA CX, et non dans la configuration ASA. Vous devrez également définir des paramètres réseau supplémentaires au niveau de l'interface de ligne de commande ASA CX. Consultez le guide de démarrage rapide d'ASA CX pour obtenir des renseignements sur cet écran.

Configuration de base ASA FirePOWER

Vous pouvez utiliser Startup Wizard (Assistant de démarrage) dans ASDM pour configurer les informations d'adresse de gestion d'ASA FirePOWER et accepter le contrat de licence d'utilisateur final (EULA). Ces paramètres sont enregistrés dans la configuration ASA FirePOWER, et non dans la configuration ASA. Vous devrez également configurer certains paramètres dans l'interface de ligne de commande d'ASA FirePOWER. Pour en savoir plus, consultez le chapitre sur le module ASA FirePOWER dans le guide de configuration de pare-feu.

Configuration du fuseau horaire et de l'horloge

Configurez les paramètres de l'horloge.

Serveur de mise à jour automatique (mode unique)

Suivez ces lignes directrices pour configurer un serveur de mise à jour automatique :

- Configurez un serveur de mise à jour automatique en cochant la case **Enable Auto Update Server for ASA** (Activer le serveur de mise à jour automatique pour l'ASA).

- Cochez la case **Enable Signature and Engine Updates from Cisco.com** (Activer les mises à jour des signatures et du moteur depuis Cisco.com) si vous avez un module IPS. Définissez les paramètres supplémentaires suivants :
  - Saisissez votre nom d'utilisateur et mot de passe, puis confirmez le mot de passe.
  - Saisissez l'heure de début au format hh:mm:ss, en utilisant une horloge de 24 heures.

Résumé de l'assistant de démarrage

Cet écran résume tous les paramètres de configuration que vous avez définis pour l'ASA.

- Cliquez sur **Back** (Retour) pour modifier les paramètres dans les écrans précédents.
- Effectuez l'une des opérations suivantes :
  - Si vous avez exécuté l'assistant de démarrage directement à partir d'un navigateur, lorsque vous cliquez sur **Finish** (Terminer), les paramètres de configuration que vous avez créés à l'aide de l'assistant sont envoyés à l'appareil de sécurité adaptable Cisco et enregistrés automatiquement dans la mémoire flash.
  - Si vous avez exécuté l'assistant de démarrage à partir d'ASDM, vous devez enregistrer explicitement la configuration dans la mémoire flash en choisissant **File (Fichier) > Save Running Configuration to Flash (Enregistrer la configuration en cours d'exécution dans la mémoire flash).**

Historique de l'assistant de démarrage

Tableau 13 : Historique de l'assistant de démarrage

Nom de la caractéristique	Versions de plateforme	Description
Assistant de démarrage	7.0(1)	Cet assistant a été introduit. Nous avons lancé l'écran **Wizards (Assistants) > Startup Wizard (Assistant de démarrage)**.
Configuration IPS ASA	v 8.4(1)	Pour le module IPS ASA, l'écran **Configuration de base IPS** a été ajouté à l'assistant de démarrage. Les mises à jour de signatures pour le module IPS ont également été ajoutées à l'écran **Mise à jour automatique**. L'écran **Configuration du fuseau horaire et de l'horloge** a été ajouté pour vérifier que l'horloge est réglée sur l'ASA; le module IPS obtient son horloge de l'ASA. Nous avons introduit ou modifié les écrans suivants : **Assistants > Assistant de démarrage > Configuration de base IPS** **Assistants > Assistant de démarrage > Mise à jour automatique** **Assistants > Assistant de démarrage > Configuration du fuseau horaire et de l'horloge**

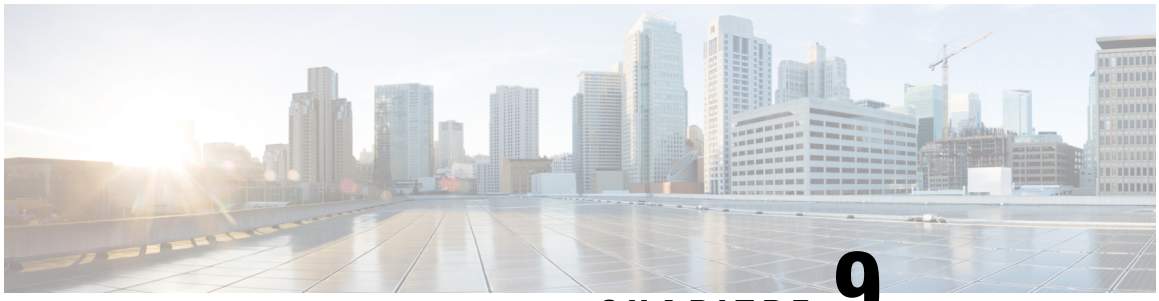
Nom de la caractéristique	Versions de plateforme	Description
Configuration ASA CX	9.1(1)	Pour le module ASA CX, l'écran **Configuration de base ASA CX** a été ajouté à l'assistant de démarrage. Nous avons introduit les écrans suivants : **Assistants > Assistant de démarrage > Configuration de base ASA CX**
Configuration ASA FirePOWER	9.2(2.4)	Pour le module ASA FirePOWER, l'écran **Configuration de base ASA FirePOWER** a été ajouté à l'assistant de démarrage. Nous avons introduit les écrans suivants : **Assistants > Assistant de démarrage > Configuration de base ASA FirePOWER**



PARTIE II

Fonctionnalités de haute disponibilité et d'évolutivité

- Mode contexte multiple, à la page 255
- Basculement pour la haute disponibilité, à la page 293
- Basculement pour la haute disponibilité dans le nuage public, à la page 345
- Grappe ASA pour le Secure Firewall 3100, à la page 363
- Grappe ASA pour le Firepower 4100/9300, à la page 451
- Grappe ASA pour l'ASA virtuel pour le cloud privé, à la page 547



CHAPITRE 9

Mode contexte multiple

Ce chapitre décrit comment configurer plusieurs contextes de sécurité sur l'ASA.

- À propos des contextes de sécurité, à la page 255
- Licences pour le mode de contexte multiple, à la page 267
- Conditions préalables pour le mode de contexte multiple, à la page 268
- Lignes directrices pour le mode de contexte multiple, à la page 268
- Paramètres par défaut du mode de contexte multiple, à la page 269
- Configurer plusieurs contextes, à la page 269
- Changer entre les contextes et l'espace d'exécution du système, à la page 280
- Gérer les contextes de sécurité, à la page 280
- Supervision des contextes de sécurité, à la page 284
- Historique du mode de contexte multiple, à la page 287

À propos des contextes de sécurité

Vous pouvez partitionner un ASA unique en plusieurs périphériques virtuels, appelés contextes de sécurité. Chaque contexte agit comme un périphérique indépendant, avec sa politique de sécurité, ses interfaces et ses administrateurs. Les contextes multiples sont similaires au fait d'avoir plusieurs périphériques autonomes. Pour les fonctionnalités non prises en charge en mode de contexte multiple, consultez Lignes directrices pour le mode de contexte multiple, à la page 268.

Cette section fournit un aperçu des contextes de sécurité.

Utilisations courantes des contextes de sécurité

Vous pouvez utiliser plusieurs contextes de sécurité dans les situations suivantes :

- Vous êtes un fournisseur de services et vous souhaitez vendre des services de sécurité à de nombreux clients. En activant plusieurs contextes de sécurité sur l'ASA, vous pouvez mettre en œuvre une solution économique et peu encombrante qui sépare et sécurise tout le trafic client, tout en facilitant la configuration.
- Vous êtes une grande entreprise ou un campus universitaire et souhaitez séparer complètement les services.
- Vous êtes une entreprise qui souhaite fournir des politiques de sécurité distinctes à différents services.
- Vous avez un réseau qui nécessite plusieurs ASA.

Fichiers de configuration de contexte

Cette section décrit comment l'ASA met en œuvre les configurations en mode de contexte multiple.

Configurations de contexte

Pour chaque contexte, l'ASA comprend une configuration qui identifie la politique de sécurité, les interfaces et toutes les options que vous pouvez configurer sur un périphérique autonome. Vous pouvez stocker les configurations de contexte dans la mémoire flash ou vous pouvez les télécharger à partir d'un serveur TFTP, FTP ou HTTP(S).

Configuration système

L'administrateur du système ajoute et gère les contextes en configurant chaque emplacement de configuration de contexte, les interfaces allouées et d'autres paramètres de fonctionnement de contexte dans la configuration système, qui, à l'instar d'une configuration monomode, est la configuration de démarrage. La configuration système identifie les paramètres de base de l'ASA. La configuration système n'inclut aucune interface réseau ni aucun paramètre réseau pour elle-même; au contraire, lorsque le système doit accéder à des ressources réseau (comme le téléchargement des contextes à partir du serveur), il utilise l'un des contextes désigné comme *contexte d'administration*. La configuration système comprend une interface de basculement spécialisée pour le trafic de basculement uniquement.

Configuration du contexte d'administration

Le contexte d'administration est similaire à tout autre contexte, sauf que lorsqu'un utilisateur se connecte au contexte d'administration, cet utilisateur dispose de droits d'administrateur système et peut accéder au système et à tous les autres contextes. Le contexte admin n'est limité en aucune façon et peut être utilisé comme contexte standard. Cependant, comme la connexion au contexte admin vous accorde des privilèges d'administrateur sur tous les contextes, vous devrez peut-être restreindre l'accès au contexte admin aux utilisateurs appropriés. Le contexte d'administration doit résider dans la mémoire flash et non à distance.

Si votre système est déjà en mode de contexte multiple, ou si vous effectuez une conversion à partir du mode unique, le contexte d'administration est automatiquement créé sous la forme d'un fichier sur la mémoire flash interne, appelé admin.cfg. Ce contexte s'appelle « admin ». Si vous ne souhaitez pas utiliser admin.cfg comme contexte d'administration, vous pouvez modifier le contexte d'administration.

Classement des paquets par l'ASA

Chaque paquet qui entre dans le châssis doit être classé par l'ASA, de sorte que ce dernier puisse déterminer à quel contexte envoyer un paquet.



Remarque Si l'adresse MAC de destination est une adresse MAC de multidiffusion ou de diffusion, le paquet est dupliqué et remis à chaque contexte.

Critères de classificateurs valides

Cette section décrit les critères utilisés par le classificateur.

Remarque Pour le trafic de gestion destiné à une interface, l'adresse IP de l'interface est utilisée pour la classification.

La table de routage n'est pas utilisée pour la classification des paquets.

Interfaces uniques

Si un seul contexte est associé à l'interface d'entrée, l'ASA classe le paquet dans ce contexte. En mode de pare-feu transparent, des interfaces uniques pour les contextes sont requises. Cette méthode est donc utilisée pour classer les paquets à tout moment.

Adresses MAC uniques

Si plusieurs contextes partagent une interface, le classificateur utilise des adresses MAC uniques attribuées à l'interface dans chaque contexte. Un routeur en amont ne peut pas acheminer directement vers un contexte sans adresse MAC unique. Vous pouvez activer la génération automatique des adresses MAC. Vous pouvez également définir les adresses MAC manuellement lorsque vous configurez chaque interface.

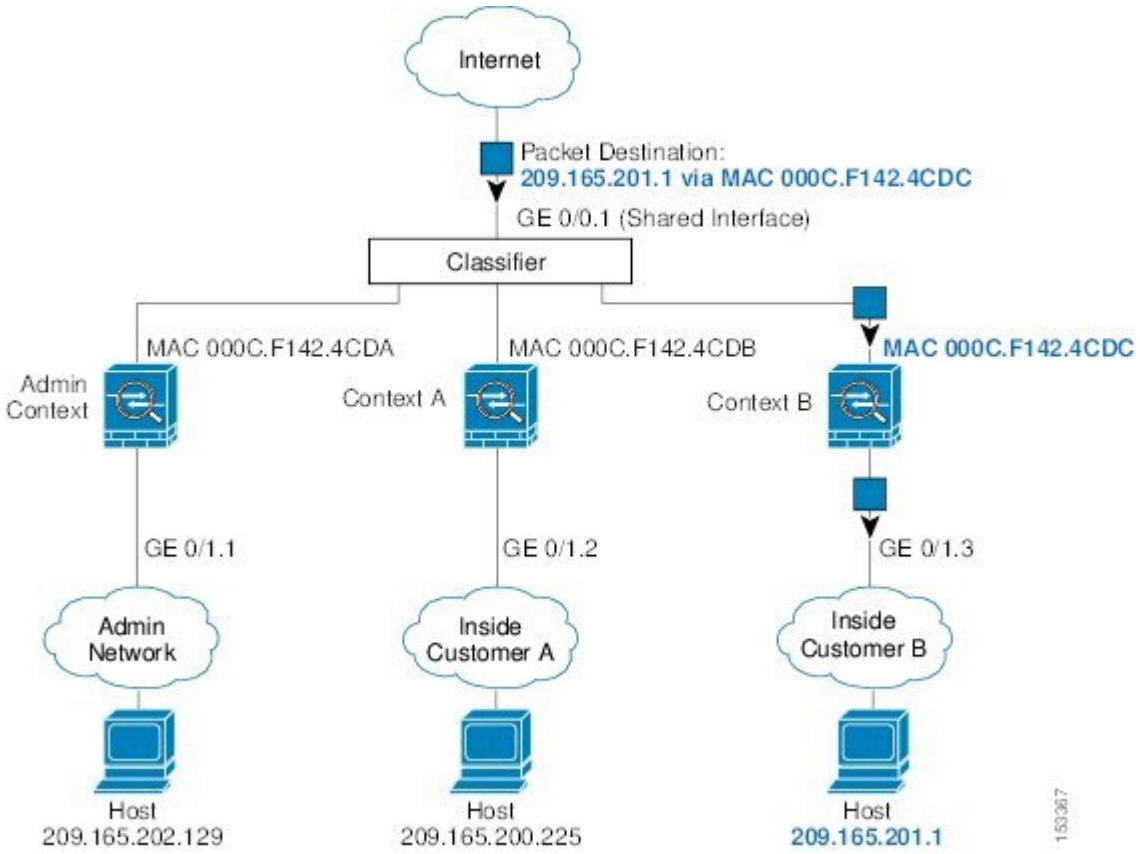
Configuration NAT

Si vous n'activez pas l'utilisation d'adresses MAC uniques, l'ASA utilise les adresses mappées dans votre configuration NAT pour classer les paquets. Nous vous conseillons d'utiliser des adresses MAC au lieu de NAT afin que la classification du trafic puisse avoir lieu indépendamment de l'exhaustivité de la configuration NAT.

Exemples de classement

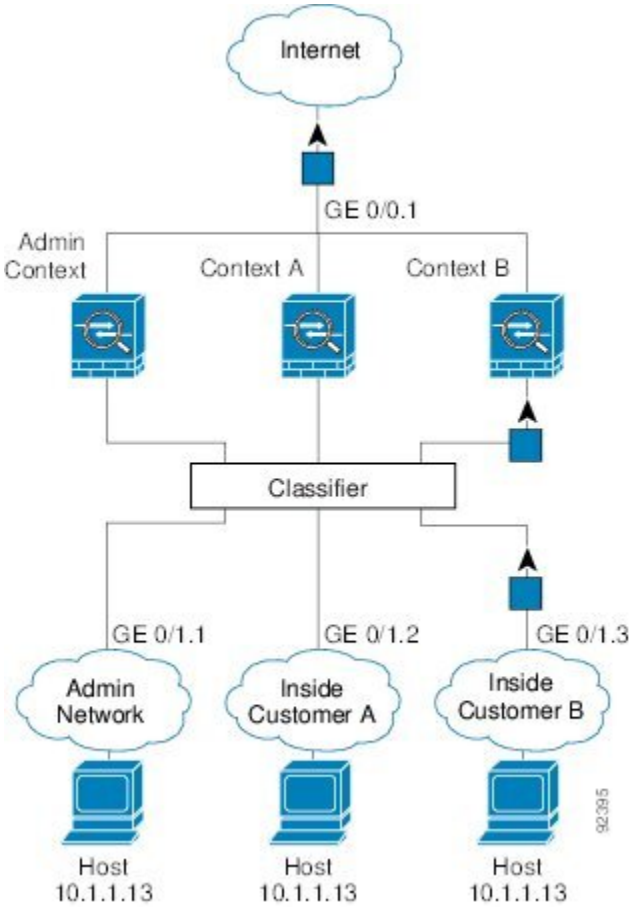
La figure suivante montre plusieurs contextes partageant une interface externe. Le classificateur affecte le paquet au contexte B, car le contexte B comprend l'adresse MAC à laquelle le routeur envoie le paquet.

Illustration 42 : Classification des paquets avec une interface partagée à l'aide d'adresses MAC



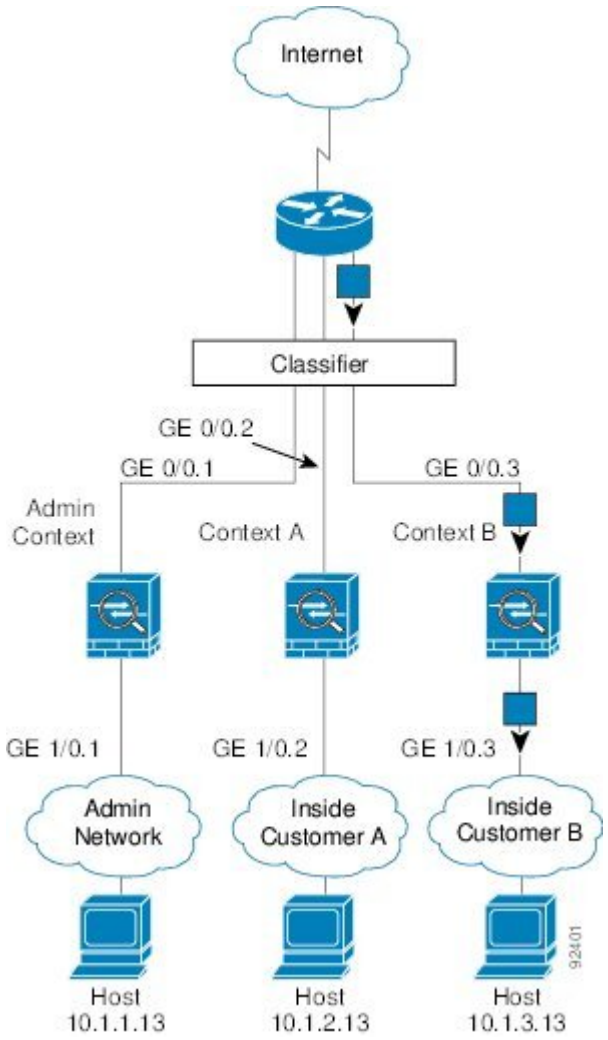
Notez que tout nouveau trafic entrant doit être classé, même en provenance des réseaux internes. La figure suivante montre un hôte sur le réseau interne du contexte B qui accède à Internet. Le classificateur affecte le paquet au contexte B, car l'interface d'entrée est Gigabit Ethernet 0/1.3, qui est affectée au contexte B.

Illustration 43 : Trafic entrant des réseaux internes



Pour les pare-feu transparents, vous devez utiliser des interfaces uniques. La figure suivante montre un paquet destiné à un hôte du contexte B à partir d'Internet. Le classificateur affecte le paquet au contexte B, car l'interface d'entrée est Gigabit Ethernet 1/0.3, qui est affectée au contexte B.

Illustration 44 : Contextes de pare-feu transparent



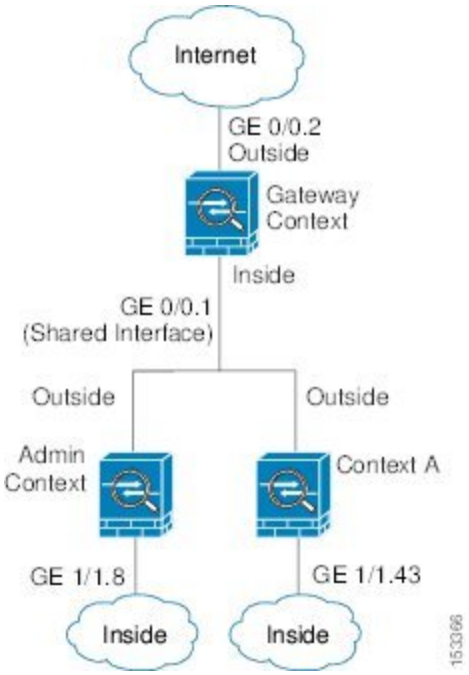
Contextes de sécurité en cascade

Le fait de placer un contexte directement devant un autre contexte s'appelle *des contextes en cascade*; l'interface externe d'un contexte est la même interface que l'interface interne d'un autre contexte. Vous pourriez souhaiter mettre des contextes en cascade si vous souhaitez simplifier la configuration de certains contextes en configurant des paramètres partagés dans le contexte supérieur.

Remarque La mise en cascade des contextes nécessite des adresses MAC uniques pour chaque interface de contexte. En raison des limites de la classification des paquets sur des interfaces partagées sans adresses MAC, nous vous conseillons de ne pas utiliser de contextes de chaîne de caractères sans adresses MAC uniques.

La figure suivante montre un contexte de passerelle avec deux contextes derrière la passerelle.

Illustration 45 : Contextes en cascade



Accès de gestion aux contextes de sécurité

L'ASA fournit un accès administrateur de système en mode de contexte multiple ainsi qu'un accès pour les administrateurs de contexte individuel.

Accès à l'administrateur système

Vous pouvez accéder à l'ASA en tant qu'administrateur système de deux manières :

- Accédez à la console ASA.

  À partir de la console, vous accédez à l'*espace d'exécution du système*, ce qui signifie que toutes les commandes que vous saisissez n'affectent que la configuration ou le fonctionnement du système (pour les commandes d'exécution).

- Accédez au contexte d'administration à l'aide de Telnet, SSH ou ASDM.

En tant qu'administrateur système, vous pouvez accéder à tous les contextes.

L'espace d'exécution du système ne prend en charge aucune commande AAA, mais vous pouvez configurer son propre mot de passe d'activation, ainsi que ses noms d'utilisateur dans la base de données locale pour fournir des connexions individuelles.

Accès à l'administrateur de contexte

Vous pouvez accéder à un contexte en utilisant Telnet, SSH ou ASDM. Si vous vous connectez à un contexte de non-administration, vous pouvez uniquement accéder à la configuration de ce contexte. Vous pouvez fournir des identifiants individuels pour le contexte.

Utilisation de l'interface de gestion

L'interface de gestion est une interface distincte uniquement pour le trafic de gestion.

En mode de pare-feu routé, vous pouvez partager l'interface de gestion dans tous les contextes.

En mode de pare-feu transparent, l'interface de gestion est spéciale. En plus du nombre maximal d'interfaces de trafic traversant autorisé, vous pouvez également utiliser l'interface de gestion en tant qu'interface de gestion uniquement distincte. Cependant, en mode contexte multiple, vous ne pouvez pas partager d'interfaces entre des contextes transparents. Vous pouvez plutôt utiliser les sous-interfaces de l'interface de gestion et en affecter une à chaque contexte. Cependant, seuls les modèles de périphérique Firepower autorisent les sous-interfaces sur l'interface de gestion. Pour les modèles d'ASA, vous devez utiliser une interface de données ou une sous-interface d'une interface de données et l'ajouter à un groupe de ponts dans le contexte.

Pour le contexte transparent Châssis Firepower 4100/9300 , ni l'interface de gestion ni la sous-interface ne conservent leur état spécial. Dans ce cas, vous devez la traiter comme une interface de données et l'ajouter à un groupe de ponts. (Notez qu'en mode contexte unique, l'interface de gestion conserve son état spécial.)

Une autre considération à propos du mode transparent : lorsque vous activez le mode à contextes multiples, toutes les interfaces configurées sont automatiquement affectées au contexte Admin. Par exemple, si votre configuration par défaut comprend l'interface de gestion, cette interface sera affectée au contexte d'administration. Une option consiste à laisser l'interface principale allouée au contexte d'administration et à la gérer à l'aide du VLAN natif, puis d'utiliser des sous-interfaces pour gérer chaque contexte. Gardez à l'esprit que si vous rendez le contexte d'administration transparent, son adresse IP sera supprimée. Vous devez l'affecter à un groupe de ponts et affecter l'adresse IP aux BVI.

À propos de la gestion des ressources

Par défaut, tous les contextes de sécurité ont un accès illimité aux ressources de l'ASA, sauf lorsque des limites maximales par contexte sont appliquées; la seule exception concerne les ressources du VPN, qui sont désactivées par défaut. Si vous trouvez qu'un ou plusieurs contextes utilisent trop de ressources et qu'ils entraînent le refus de connexion à d'autres contextes, par exemple, vous pouvez configurer la gestion des ressources pour limiter l'utilisation des ressources par contexte. Pour les ressources VPN, vous devez configurer la gestion des ressources pour autoriser tous les tunnels VPN.

Classes des ressources

L'ASA gère les ressources en attribuant des contextes aux classes de ressources. Chaque contexte utilise les limites de ressources définies par la classe. Pour utiliser les paramètres d'une classe, affectez le contexte à la classe lorsque vous définissez le contexte. Tous les contextes appartiennent à la classe par défaut s'ils ne sont pas affectés à une autre classe; vous n'avez pas à attribuer activement un contexte à la classe par défaut. Vous ne pouvez affecter un contexte qu'à une seule classe de ressources. L'exception à cette règle est que les limites non définies dans la classe membre sont héritées de la classe par défaut; ainsi, un contexte peut être membre de la classe par défaut et d'une autre classe.

Limites des ressources

Vous pouvez définir la limite des ressources individuelles en pourcentage (s'il y a une limite de système matériel) ou en tant que valeur absolue.

Pour la plupart des ressources, l'ASA ne réserve pas une partie des ressources pour chaque contexte attribué à la classe; au lieu de cela, l'ASA définit la limite maximum pour un contexte. Si vous dépassez les ressources ou si vous permettez à certaines ressources d'être illimitées, quelques contextes peuvent « utiliser » ces ressources, ce qui peut affecter le service fourni à d'autres contextes. L'exception concerne les types de

ressources VPN, que vous ne pouvez pas dépasser, de sorte que les ressources attribuées à chaque contexte sont garanties. Pour prendre en charge des rafales temporaires de sessions VPN au-delà de la quantité attribuée, l'ASA prend en charge un type de ressource VPN en « rafale », qui est égal au nombre de sessions VPN non attribuées restantes. Les sessions en rafale *peuvent* être surexploitées et sont disponibles pour les contextes selon le principe du premier arrivé premier servi.

Classe par défaut

Tous les contextes appartiennent à la classe par défaut s'ils ne sont pas affectés à une autre classe; vous n'avez pas besoin d'affecter activement un contexte à la classe par défaut.

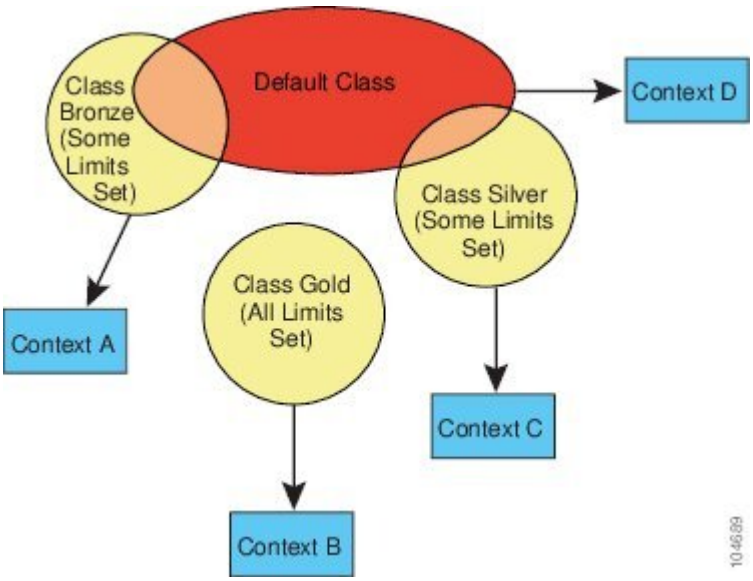
Si un contexte appartient à une autre classe que la classe par défaut, les paramètres de cette classe remplacent toujours les paramètres de la classe par défaut. Cependant, si l'autre classe a des paramètres non définis, le contexte membre utilise la classe par défaut pour ces limites. Par exemple, si vous créez une classe avec une limite de 2 % pour toutes les connexions simultanées, mais aucune autre limite, toutes les autres limites sont héritées de la classe par défaut. Inversement, si vous créez une classe avec une limite pour toutes les ressources, la classe n'utilise aucun paramètre de la classe par défaut.

Pour la plupart des ressources, la classe par défaut fournit un accès illimité aux ressources pour tous les contextes, sauf pour les limites suivantes :

- Sessions Telnet—5 sessions. (Le maximum par contexte.)
- Sessions SSH—5 sessions. (Le maximum par contexte.)
- Sessions ASDM—5 sessions. (Le maximum par contexte.)
- Adresses MAC—(selon le modèle). (Le maximum pour le système.)
- Secure Client (services client sécurisés) homologues—0 session. (Vous devez configurer manuellement la classe pour autoriser tous les homologues Secure Client (services client sécurisés).)
- Tunnels VPN de site à site—0 session. (Vous devez configurer manuellement la classe pour autoriser toutes les sessions VPN.)

La figure suivante montre la relation entre la classe par défaut et les autres classes. Les contextes A et C appartiennent à des classes avec des limites définies; les autres limites sont héritées de la classe par défaut. Le contexte B n'hérite aucune limite de la valeur par défaut, car toutes les limites sont définies dans sa classe, la classe Gold. Le contexte D n'a pas été affecté à une classe et est, par défaut, membre de la classe par défaut.

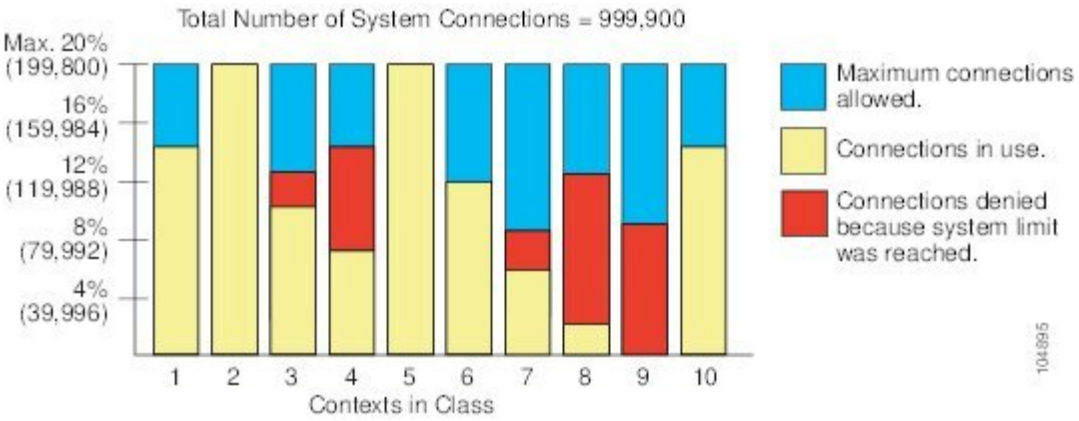
Illustration 46 : Classes des ressources



Utiliser des ressources surexploitées

Vous pouvez surabonner l'ASA en attribuant plus de 100 % d'une ressource dans tous les contextes (à l'exception des ressources VPN non rafales). Par exemple, vous pouvez définir la classe bronze pour limiter les connexions à 20 % par contexte, puis affecter 10 contextes à la classe pour un total de 200 %. Si les contextes utilisent simultanément plus que la limite du système, chaque contexte obtient moins des 20 % prévus.

Illustration 47 : Surabonnement des ressources

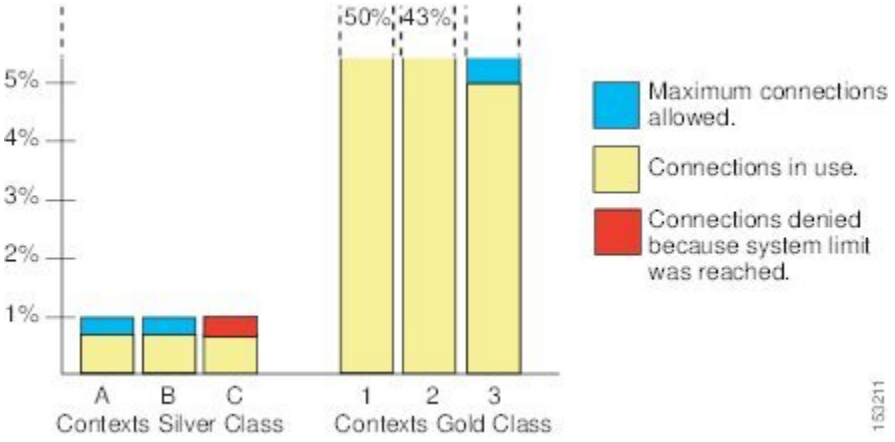


Utiliser des ressources illimitées

L'ASA vous permet d'attribuer un accès illimité à une ou plusieurs ressources dans une classe, au lieu d'un pourcentage ou d'un nombre absolu. Lorsqu'une ressource est illimitée, les contextes peuvent utiliser autant de ressources que le système en dispose. Par exemple, les contextes A, B et C appartiennent à la classe Silver, qui limite chaque membre de la classe à 1 % des connexions, pour un total de 3 %; mais les trois contextes n'utilisent actuellement que 2 % combinés. La classe Gold dispose d'un accès illimité aux connexions. Les

contextes de la classe Gold peuvent utiliser plus de 97 % des connexions « non attribuées »; ils peuvent également utiliser le 1 % de connexions non actuellement utilisées par les contextes A, B et C, même si cela signifie que les contextes A, B et C ne peuvent pas atteindre leur limite combinée de 3 %. La configuration d'un accès illimité s'apparente au surabonnement de l'ASA, à la différence que vous avez moins de contrôle sur le nombre de surabonnements du système.

Illustration 48 : Ressources illimitées



À propos des adresses MAC

Vous pouvez affecter manuellement des adresses MAC pour remplacer la valeur par défaut. Pour le mode de contexte multiple, vous pouvez générer automatiquement des adresses MAC uniques (pour toutes les interfaces affectées à un contexte) et un mode de contexte unique (pour les sous-interfaces).

Remarque Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur ASA, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de liaison IPv6 sont générées sur la base de l'adresse MAC, l'attribution d'adresses MAC uniques aux sous-interfaces permet d'obtenir des adresses locales de liaison IPv6 uniques, ce qui peut éviter la perturbation du trafic dans certaines instances du périphérique ASA.

Adresses MAC en mode de contexte multiple

L'adresse MAC est utilisée pour classer les paquets dans un contexte. Si vous partagez une interface, mais que vous n'avez pas d'adresses MAC uniques pour l'interface dans chaque contexte, d'autres méthodes de classification sont tentées qui pourraient ne pas fournir une couverture complète.

Pour permettre aux contextes de partager des interfaces, vous devez activer la génération automatique d'adresses MAC virtuelles pour chaque interface de contexte partagé.

Adresses MAC automatiques

En mode de contexte multiple, la génération automatique affecte des adresses MAC uniques à toutes les interfaces affectées à un contexte.

Si vous attribuez manuellement une adresse MAC et activez la génération automatique, l'adresse MAC attribuée manuellement est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement est utilisée, si elle est activée.

Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC pour l'interface.

Comme les adresses générées automatiquement (lors de l'utilisation d'un préfixe) commencent par A2, vous ne pouvez pas commencer les adresses MAC manuelles par A2 si vous souhaitez également utiliser la génération automatique.

Le châssis génère l'adresse MAC en utilisant le format suivant :

A2*xx.yyzz.zzzz*

Où *xx.yy* est un préfixe défini par l'utilisateur ou un préfixe généré automatiquement en fonction des deux derniers octets de l'adresse MAC de l'interface, et *zz.zzzz* est un compteur interne généré par l'ASA. Pour l'adresse MAC de secours, l'adresse est identique, sauf que le compteur interne est augmenté de 1.

Pour donner un exemple d'utilisation du préfixe, si vous définissez le préfixe 77, l'ASA convertit 77 en valeur hexadécimale 004D (*yyxx*). Lorsqu'il est utilisé dans l'adresse MAC, le préfixe est inversé (*xxyy*) pour correspondre à la forme native de l'ASA :

A2**4D.00***zz.zzzz*

Pour un préfixe 1009 (03F1), l'adresse MAC est :

A2**F1.03***zz.zzzz*

Remarque Le format d'adresse MAC sans préfixe est une version existante. Consultez la commande **mac-address auto** dans la référence de commandes pour plus d'informations sur le format existant.

Prise en charge du VPN

Pour les ressources VPN, vous devez configurer la gestion des ressources pour autoriser tous les tunnels VPN.

Vous pouvez utiliser le VPN de site à site en mode de contexte multiple.

Pour le VPN d'accès à distance, vous devez utiliser AnyConnect 3.x ou une version ultérieure pour le SSL VPN et le protocole IKEv2. Vous pouvez personnaliser le stockage flash par contexte pour les images et les personnalisations Secure Client (services client sécurisés), et utiliser la mémoire flash partagée pour tous les contextes. Pour les fonctionnalités non prises en charge, consultez Lignes directrices pour le mode de contexte multiple, à la page 268. Pour une liste détaillée des fonctionnalités VPN prises en charge par version ASA, consultez Historique du mode de contexte multiple, à la page 287.

Remarque La licence Secure Client Premier est requise pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante.

Licences pour le mode de contexte multiple

Modèle	Exigence de licence
Firepower 1010	Aucune assistance.
Firepower 1100	Licence Essentials : 2 contextes. *Licence facultative, maximum :* *Firepower 1120 : 5* *Firepower 1140 : 10* *Firepower 1150 : 25*
Firepower de la série 2100	Licence Essentials : 2 contextes. *Licence facultative, maximum :* *Firepower 2110 : 25* *Firepower 2120 : 25* *Firepower 2130 : 30* *Firepower 2140 : 40*
Secure Firewall 3100	Licence Essentials : 2 contextes. *Licence facultative, maximum :* *Secure Firewall 3105 : 100* *Secure Firewall 3110 : 100* *Secure Firewall 3120 : 100* *Secure Firewall 3130 : 100* *Secure Firewall 3140 : 100*
Firepower 4100	Licence Essentials : 10 contextes. *Licence facultative : jusqu'à 250 contextes.*
Firepower 9300	Licence Essentials : 10 contextes. *Licence facultative : jusqu'à 250 contextes.*
ISA 3000	Aucune assistance.
ASA virtuel	Aucune assistance.

Remarque Si le contexte d'administration ne contient que des interfaces de gestion uniquement et ne comprend aucune interface de données pour le trafic de transit, il n'est pas pris en compte dans la limite.

Remarque La licence Secure Client Premier est requise pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante.

Conditions préalables pour le mode de contexte multiple

Une fois que vous êtes en mode de contexte multiple, connectez-vous auau contexte d'administration pour accéder à la configuration système. Vous ne pouvez pas configurer le système à partir d'un contexte de non-administration. Par défaut, après avoir activé le mode de contexte multiple, vous pouvez vous connecter au contexte d'administration en utilisant l'adresse IP de gestion par défaut.

Lignes directrices pour le mode de contexte multiple

Basculement

Le basculement en mode actif/actif n'est pris en charge qu'en mode de contexte multiple.

IPv6

Le routage IPv6 inter-contextes n'est pas pris en charge.

Fonctionnalités non prises en charge

Le mode de contexte multiple ne prend pas en charge les fonctionnalités suivantes :

- RIP
- OSPFv3. (OSPFv2 est pris en charge.)
- Routage multidiffusion
- Détection des menaces
- Communications unifiées
- Qualité de service
- Interfaces de tunnel virtuel (VTI)
- Suivi du routage statique

Le mode de contexte multiple ne prend actuellement pas en charge les fonctionnalités suivantes pour le VPN d'accès à distance :

- AnyConnect 2.x et versions antérieures
- IKEv1
- SAML
- Lancement Web

- Mise en correspondance VLAN
- Analyse de l'hôte
- Équilibrage de la charge VPN
- Personnalisation
- L2TP

Directives supplémentaires

- Le mode de contexte (unique ou multiple) n'est pas stocké dans le fichier de configuration, même s'il résiste aux redémarrages. Si vous devez copier votre configuration sur un autre périphérique, définissez le mode sur le nouveau périphérique pour qu'il corresponde.
- Si vous stockez les configurations de contexte dans le répertoire racine de la mémoire flash, sur certains modèles, vous risquez de manquer d'espace dans ce répertoire, même s'il y a de la mémoire disponible. Dans ce cas, créez un sous-répertoire pour vos fichiers de configuration. Arrière-plan : certains modèles utilisent le système de fichiers FAT 16 pour la mémoire flash interne, et si vous n'utilisez pas les noms abrégés conformes à la norme 8.3 ou les caractères majuscules, moins de 512 fichiers et dossiers peuvent être stockés parce que le système de fichiers utilise des logements pour stocker les noms de fichiers longs (voir https://support.microsoft.com).
- Dans ACI, le contrôle d'intégrité de la redirection basée sur les politiques (PBR) est exécuté (pings L2) en utilisant la même adresse MAC sur toutes les feuilles. Cela entraîne une oscillation MAC. Pour résoudre l'oscillation MAC, vous pouvez configurer l'option tap-mode sur l'ensemble en ligne. Cependant, si le Firewall Threat Defense à haute disponibilité est configuré, vous devez activer l'apprentissage MAC pour la gestion des connexions lors d'un basculement. Ainsi, dans un environnement ACI avec Firewall Threat Defense dans une paire à haute disponibilité utilisant des interfaces d'ensemble en ligne, pour éviter les pertes de paquet, déployez Firewall Threat Defense en mode autonome ou dans une grappe.

Paramètres par défaut du mode de contexte multiple

- Par défaut, l'ASA est en mode de contexte unique.
- Consultez Classe par défaut, à la page 263.

Configurer plusieurs contextes

Procédure

Étape 1 Activer ou désactiver le mode de contexte multiple, à la page 270.

Étape 2 (Facultatif) Configurer une classe pour la gestion des ressources, à la page 272

Remarque Pour la prise en charge VPN, vous devez configurer des ressources VPN dans une classe de ressources; la classe par défaut n'autorise pas le VPN.

Étape 3 Configurez les interfaces dans l'espace d'exécution du système.

- Firepower 1100, Firepower 2100 en mode Appliance (appareil), Secure Firewall 3100 -Configuration de l'interface de base, à la page 611.
- Firepower 2100 en mode plateforme : consultez le guide de démarrage.
- Firepower 4100/9300—Périphériques logiques pour le Firepower 4100/9300, à la page 199

Étape 4 Configurer un contexte de sécurité, à la page 276.

Étape 5 (Facultatif) Attribuer automatiquement des adresses MAC aux interfaces de contexte, à la page 279

Étape 6 Terminez la configuration de l'interface dans le contexte. Consultez Interfaces en mode routage et en mode transparent, à la page 693.

Activer ou désactiver le mode de contexte multiple

Votre ASA est peut-être déjà configuré pour plusieurs contextes de sécurité selon la façon dont vous l'avez commandé auprès de Cisco. Si vous devez passer du mode unique au mode multiple, suivez les procédures de cette section.

ASDM prend en charge le changement de mode, du mode unique au mode multiple, si vous utilisez l'assistant de haute disponibilité et d'évolutivité et que vous activez le basculement actif/actif. Consultez Basculement pour la haute disponibilité, à la page 293 pour de plus amples renseignements. Si vous ne souhaitez pas utiliser le basculement actif/actif ou si vous souhaitez revenir en mode unique, vous devez changer de mode à l'aide de l'interface de ligne de commande; Comme le changement de mode nécessite une confirmation, vous ne pouvez pas utiliser l'outil de l'interface de ligne de commande. Cette section décrit les changements de mode au niveau de l'interface de ligne de commande.

Activer le mode de contexte multiple

Lorsque vous passez du mode unique au mode multiple, l'ASA convertit la configuration d'exécution en deux fichiers : une nouvelle configuration de démarrage qui comprend la configuration système et admin.cfg qui comprend le contexte d'administration (dans le répertoire racine de la mémoire flash interne). La configuration d'exécution d'origine est enregistrée sous le nom old_running.cfg (dans le répertoire racine de la mémoire flash interne). La configuration de démarrage d'origine n'est pas enregistrée. L'ASA ajoute automatiquement une entrée pour le contexte d'administration à la configuration système avec le nom « administration ».

Avant de commencer

Sauvegardez votre configuration de démarrage si elle diffère de la configuration d'exécution. Lorsque vous passez du mode unique au mode multiple, l'ASA convertit la configuration d'exécution en deux fichiers. La configuration de démarrage d'origine n'est pas enregistrée. Voir Gérer les fichiers, à la page 1193.

Procédure

Passez en mode de contexte multiple.

mode multiple

Exemple :

Vous êtes invité à changer de mode et à convertir la configuration, puis le système se recharge.



Remarque Vous devrez régénérer la paire de clés RSA dans le contexte d'administration avant de pouvoir rétablir une connexion SSH. Dans la console, saisissez la commande **crypto key generate rsa modulus**. Consultez Configurer l'accès SSH, à la page 1138 pour de plus amples renseignements.

Exemple :

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

Converting the configuration - this may take several minutes for a large configuration

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple
ciscoasa(config)#


***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   change mode
Shutting down isakmp
Shutting down webvpn
Shutting down License Controller
Shutting down File system



***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
```

Rétablir le mode de contexte unique

Pour copier l'ancienne configuration en cours d'exécution dans la configuration de démarrage et changer le mode en mode unique, procédez comme suit.

Avant de commencer

Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Copiez la version de sauvegarde de votre configuration d'origine en cours d'exécution dans la configuration de démarrage actuelle :

copy disk0:old_running.cfg startup-config

Exemple :

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

Étape 2 Définissez le mode en mode unique :

mode unique

Exemple :

```
ciscoasa(config)# mode single
```

Vous êtes invité à redémarrer l'ASA.

Configurer une classe pour la gestion des ressources

Pour configurer une classe dans la configuration système, procédez comme suit. Vous pouvez modifier la valeur d'une limite de ressource particulière en entrant la commande avec une nouvelle valeur.

Avant de commencer

- Exécutez cette procédure dans l'espace d'exécution du système.
- Le tableau suivant répertorie les types de ressources et leurs limites.



Remarque Si la limite du système est S.O., vous ne pouvez pas définir de pourcentage de la ressource, car il n'y a pas de limite de système stricte pour la ressource.

Tableau 14 : Noms et limites des ressources

Nom de la ressource	Taux ou simultané	Nombre minimal et maximal par contexte	Limite du système	Description
Sessions ASDM	Simultané	Au moins 1 5 au maximum	200	Sessions de gestion ASDM Les sessions ASDM utilisent deux connexions HTTPS: une pour la surveillance qui est toujours présente et une pour apporter des modifications de configuration qui est présente uniquement lorsque vous apportez des modifications. Par exemple, la limite système de 200 sessions ASDM représente une limite de 400 sessions HTTPS.
Connexions Connexions/sec	Simultané ou taux	S. O.	Connexions simultanées : consultez Licences par modèle, à la page 178 pour connaître la limite de connexions disponibles correspondant à votre modèle. Taux : S.O.	Connexions TCP ou UDP entre deux hôtes, y compris les connexions entre un hôte et plusieurs autres hôtes. **Remarque** Des messages syslog sont générés pour la limite la plus basse, xlates ou conns. Par exemple, si vous définissez la limite de xlates à 7 et le conns à 9, alors l'ASA génère uniquement le message syslog 321001 (« Resource xlates » limite de 7 atteinte pour le contexte « ctx1 ») et non 321002 (« Resource « conn rate » limite de 5 atteinte pour le contexte « ctx1 »).
Hôtes	Simultané	S. O.	s.o.	Les hôtes pouvant se connecter par l'intermédiaire de l'ASA.
Inspections/sec	Taux	s.o.	s.o.	nombre d'inspections d'applications par seconde
Entrées MAC	Simultané	S. O.	(varie selon le modèle)	Pour le mode de pare-feu transparent, le nombre d'adresses MAC autorisées dans le tableau d'adresses MAC.
Routes	Simultané	S. O.	s.o.	routes dynamiques.

Nom de la ressource	Taux ou simultané	Nombre minimal et maximal par contexte	Limite du système	Description
Rafale Secure Client (services client sécurisés)	Simultané	S. O.	Les homologues premium Secure Client (services client sécurisés) correspondant à votre modèle moins la somme des sessions attribuées à tous les contextes pour Secure Client (services client sécurisés).	Le nombre de sessions Secure Client (services client sécurisés) autorisées au-delà de la quantité attribuée à un contexte avec Secure Client (services client sécurisés). Par exemple, si votre modèle prend en charge 5 000 homologues et que vous affectez 4 000 homologues dans tous les contextes avec Secure Client (services client sécurisés), les 1 000 sessions restantes sont disponibles pour Burst Secure Client (services client sécurisés). Contrairement à Secure Client (services client sécurisés), qui garantit les sessions au contexte, le Secure Client (services client sécurisés) Burst peut être surabonné; le groupement de rafales est disponible pour tous les contextes selon le principe du premier arrivé, premier servi.
Secure Client (services client sécurisés)	Simultané	S. O.	Consultez Licences par modèle, à la page 178 pour connaître les homologues Premium Secure Client (services client sécurisés) disponibles correspondant à votre modèle.	Homologues Secure Client (services client sécurisés). Vous ne pouvez pas surabonner cette ressource; toutes les affectations de contexte combinées ne peuvent pas dépasser la limite du modèle. Les homologues que vous affectez pour cette ressource sont garantis par le contexte.
Autre rafale VPN	Simultané	S. O.	Le nombre de sessions Autre VPN correspondant à votre modèle moins la somme des sessions assignées à tous les contextes pour Autre VPN.	Le nombre de sessions VPN de site à site autorisées au-delà de la quantité attribuée à un contexte avec l'option Autre VPN. Par exemple, si votre modèle prend en charge 5 000 homologues et que vous affectez 4 000 homologues dans tous les contextes avec Autre VPN, les 1 000 sessions restantes sont disponibles pour Autre Rafale VPN. Contrairement à Autre VPN, qui garantit les sessions au contexte, Autre Rafale VPN peut être sursouscrit ; le groupement de rafales est disponible pour tous les contextes sur la base du premier arrivé, premier servi.

Nom de la ressource	Taux ou simultané	Nombre minimal et maximal par contexte	Limite du système	Description
Autre VPN	Simultané	S. O.	Consultez Licences de fonctionnalités prises en charge par modèle, à la page 113 pour connaître les autres sessions VPN disponibles correspondant à votre modèle.	Sessions VPN de site à site. Vous ne pouvez pas surabonner cette ressource; toutes les affectations de contexte combinées ne peuvent pas dépasser la limite du modèle. Les sessions que vous affectez pour cette ressource sont garanties par le contexte.
IKEv1 SA en négociation	Simultané (pourcentage uniquement)	S. O.	Un pourcentage des autres sessions VPN attribuée à ce contexte. Consultez les ressources Autres VPN pour attribuer des sessions au contexte.	Négociations IKEv1 SA entrantes, en tant que pourcentage de la limite du contexte de l'autre VPN.
SSH	Simultané	Au moins 1 5 au maximum	100	Séances SSH.
Stockage	Mo	Le maximum dépend du lecteur de mémoire flash que vous avez spécifié	Le maximum dépend du lecteur de mémoire flash que vous avez spécifié	Limite de stockage du répertoire de contexte en Mo.
Syslogs/sec	Taux	s.o.	s.o.	Messages syslog par seconde.
Telnet	Simultané	Au moins 1 5 au maximum	100	Sessions Telnet.
Xlates	Simultané	S. O.	s.o.	Traduction d'adresses de réseau.

Procédure

Étape 1 Si vous n'êtes pas déjà en mode de configuration système, dans le panneau **Device List (liste des périphériques)**, double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

Étape 2 Choisissez **Configuration** > **Context Management** > **Resource Class**(classe de ressources de gestion du contexte de configuration) et cliquez sur **Add**(ajouter).

La boîte de dialogue **Add Resource Class** (ajouter une classe de ressource) apparaît.

Étape 3 Saisissez un nom de classe de 20 caractères maximum dans le champ **Resource Class** (Classe de ressource).

Étape 4 Dans la zone **Count Limited Resources** (Nombre de ressources limitées), définissez les limites simultanées de ressources.

Consultez le tableau précédent pour une description de chaque type de ressource.

Pour les ressources qui n'ont pas de limite système, vous ne pouvez pas définir le pourcentage; vous ne pouvez définir qu'une valeur absolue. Si vous ne définissez pas de limite, la limite est héritée de la classe par défaut. Si la classe par défaut ne définit pas de limite, la ressource est illimitée, ou égale à la limite du système, si elle est disponible. Pour la plupart des ressources, la valeur 0 fixe la limite à illimitée. Pour les types de VPN, 0 définit la limite à Aucun.



Remarque Si vous définissez également **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Gestion des accès)** > **Management Session Quota (Gestion des quotas de sessions)** dans un contexte pour définir le nombre maximal de sessions administratives (SSH, etc.), la valeur la plus basse sera utilisée.

Étape 5 Dans la zone **Rate Limited Resource** (débit des ressources limitées), définissez la limite de débit des ressources.

Consultez le tableau précédent pour une description de chaque type de ressource.

Si vous ne définissez pas de limite, la limite est héritée de la classe par défaut. Si la classe par défaut ne définit pas de limite, elle est illimitée par défaut. 0 définit la limite à illimité.

Étape 6 Cliquez sur **OK**.

Configurer un contexte de sécurité

La définition du contexte de sécurité dans la configuration système identifie le nom du contexte, l'URL du fichier de configuration, les interfaces qu'un contexte peut utiliser et d'autres paramètres.

Avant de commencer

- Exécutez cette procédure dans l'espace d'exécution du système.
- Configurer les interfaces. Pour les contextes en mode transparent, vous ne pouvez pas partager des interfaces entre les contextes, vous pouvez donc utiliser des sous-interfaces. Pour planifier l'utilisation de l'interface de gestion, consultez Utilisation de l'interface de gestion, à la page 262.
  - Firepower 1100, Firepower 2100 en mode Appliance (appareil), Secure Firewall 3100 -Configuration de l'interface de base, à la page 611.
  - Firepower 2100 en mode plateforme : consultez le guide de démarrage.
  - Firepower 4100/9300—Périphériques logiques pour le Firepower 4100/9300, à la page 199

Procédure

Étape 1 Si vous n'êtes pas déjà en mode de configuration système, dans le panneau **Device List (liste des périphériques)**, double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

Étape 2 Choisissez **Configuration** > **Context Management (Gestion des contextes)** > **Security Contexts (Contexte de sécurité)**, puis cliquez sur **Add** (ajouter).

La boîte de dialogue**Add Context** (Ajouter un contexte) apparaît.

Étape 3 Dans le champ **Security Context** (contexte de sécurité), saisissez le nom du contexte sous la forme d'une chaîne de 32 caractères maximum.

Ce nom est sensible à la casse, vous pouvez donc avoir deux contextes nommés « clientA » et « ClientA », par exemple. « System » ou « Null » (en lettres majuscules ou minuscules) sont des noms réservés et ne peuvent pas être utilisés.

Étape 4 Dans la zone **Interface Allocation** (attribution d'interface), cliquez sur le bouton **Add** (ajouter) pour affecter une interface au contexte.

a) Dans la liste déroulante **Interfaces (interfaces)** > **Physical interfaces (interfaces physiques)**, choisissez une interface.

Vous pouvez affecter l'interface principale, auquel cas vous laissez l'ID de sous-interface vide, ou vous pouvez affecter une sous-interface ou une plage de sous-interfaces associées à cette interface. En mode transparent de pare-feu, seules les interfaces qui n'ont pas été allouées à d'autres contextes sont affichées. Si l'interface principale était déjà affectée à un autre contexte, vous devez choisir une sous-interface.

b) (Facultatif) Dans la liste déroulante **Interfaces** > **Subinterface range** (plage de sous-interfaces) choisissez un ID de sous-interface.

Pour une plage d'ID de sous-interface, choisissez l'ID de fin dans la deuxième liste déroulante, si elle est disponible.

En mode transparent de pare-feu, seules les sous-interfaces qui n'ont pas été allouées à d'autres contextes sont affichées.

c) (Facultatif) Dans la zone des **noms d'alias**, cochez la case **Use Aliased Name in Context** (Utiliser un nom d'alias dans le contexte) pour définir un nom d'alias pour cette interface à utiliser dans la configuration de contexte au lieu de l'ID de l'interface.

- Dans le champ **Name** (nom), définissez le nom d'alias.

  Un nom d'alias doit commencer par une lettre, se terminer par une lettre et avoir comme caractères internes uniquement des lettres, des chiffres ou un trait de soulignement. Ce champ vous permet de spécifier un nom qui se termine par une lettre ou un trait de soulignement; pour ajouter un chiffre facultatif après le nom, définissez le chiffre dans le champ Plage.

- (Facultatif) Dans le champ **Range** (Plage), définissez le suffixe numérique du nom d'alias.

  Si vous avez une plage de sous-interfaces, vous pouvez entrer une plage de chiffres à ajouter au nom.

d) (Facultatif) Cochez la case **Show Hardware Properties in Context** (Afficher les propriétés matérielles dans le contexte) pour permettre aux utilisateurs du contexte de voir les propriétés de l'interface physique même si vous définissez un nom d'alias.

e) Cliquez sur **OK** pour revenir à la boîte de dialogue **Add Context** (ajouter un contexte).

Étape 5 (Facultatif) Dans la zone **Resource Assignment** (Affectation des ressources), choisissez un nom de classe dans la liste déroulante **Resource Class** (Classe de ressources) pour affecter ce contexte à une classe de ressources.

Vous pouvez ajouter ou modifier une classe de ressources directement à partir de cette zone.

Étape 6 Dans la liste déroulante **Config URL** (URL de configuration), choisissez un type de système de fichiers. Dans le champ, identifiez l'URL de l'emplacement de configuration du contexte.

Par exemple, l'URL combinée pour FTP a le format suivant :

ftp://server.example.com/configs/admin.cfg

Étape 7 (Facultatif) Cliquez sur **Login** (Connexion) pour définir le nom d'utilisateur et le mot de passe pour les systèmes de fichiers externes.

Étape 8 (Facultatif) Dans la liste déroulante **Failover Group** (Groupe de basculement), choisissez le nom du groupe pour définir le groupe de basculement pour le basculement actif/actif.

Étape 9 (Facultatif) Pour **Cloud Web Security**, cliquez sur **Enable** (activer) pour activer l'inspection de Web Security dans ce contexte. Pour remplacer les licences définies dans la configuration système, saisissez une licence dans le champ **License** (Licence).

Étape 10 (Facultatif) Ajoutez une description dans le champ **Description**.

Étape 11 (Facultatif) Dans la zone **Storage URL AAssignment** (Affectation d'URL de stockage), vous pouvez autoriser chaque contexte à utiliser la mémoire flash pour stocker les paquets VPN, tels que Secure Client (services client sécurisés), ainsi que fournir le stockage pour Secure Client (services client sécurisés) et les personnalisations de portails VPN SSL sans client. Par exemple, si vous utilisez le mode de contexte multiple pour configurer un profil Secure Client (services client sécurisés) avec des politiques d'accès dynamique, vous devez planifier le stockage privé et partagé spécifique au contexte. Chaque contexte peut utiliser un espace de stockage privé ainsi qu'un espace de stockage partagé en lecture seule. **Remarque :** Assurez-vous que le répertoire cible est déjà présent sur le disque spécifié à l'aide des **outils** > **de gestion de fichiers**.

a) Cochez la case **Configure private storage assignment** (Configurer l'affectation du stockage privé) et dans la liste déroulante **Sélect** (Sélectionner), choisissez le répertoire de stockage privé. Vous pouvez spécifier un espace de stockage privé par contexte. Vous pouvez lire/écrire/supprimer à partir de ce répertoire dans le contexte (ainsi qu'à partir de l'espace d'exécution du système). Sous le chemin spécifié, l'ASA crée un sous-répertoire du nom du contexte. Par exemple, pour contexteA, si vous spécifiez **disk1:/private-storage** comme chemin, l'ASA crée un sous-répertoire pour ce contexte à l'emplacement **disk1:/private-storage/contextA/**. Vous pouvez également nommer le chemin dans le contexte en saisissant un nom dans le champ **est mappé à** afin que le système de fichiers ne soit pas rendu visible aux administrateurs de contexte. Par exemple, si vous spécifiez le nom mappé **contexte**, dans le contexte, ce répertoire est appelé **contexte:**. Pour contrôler la quantité d'espace disque autorisée par contexte, consultez Configurer une classe pour la gestion des ressources, à la page 272.

b) Cochez la case **Configure Shared Storage Affectation** (Configurer l'affectation du stockage partagé) et dans la liste déroulante **Select** (Sélectionner), choisissez le répertoire de stockage partagé. Vous pouvez spécifier un espace de stockage **shared** en lecture seule par contexte, mais vous pouvez créer plusieurs répertoires partagés. Pour réduire la duplication de fichiers volumineux communs qui peuvent être partagés dans tous les contextes, tels que les paquets Secure Client (services client sécurisés), vous pouvez utiliser l'espace de stockage partagé. L'ASA ne crée pas de sous-répertoires de contexte pour cet espace de stockage, car il s'agit d'un espace partagé par plusieurs contextes. Seul l'espace d'exécution du système peut écrire et supprimer dans le répertoire partagé.

Étape 12 Cliquez sur **OK** pour revenir au volet **Security Contexts** (Contextes de sécurité).

Étape 13 (Facultatif) Sélectionnez le contexte et cliquez sur **Change Firewall Mode** (modifier le mode de pare-feu) pour définir le mode de pare-feu transparent.

S'il s'agit d'un nouveau contexte, il n'y a aucune configuration à effacer. Cliquez sur**Change Mode** (Modifier le mode) pour passer en mode transparent de pare-feu.

S'il s'agit d'un contexte existant, veillez à sauvegarder la configuration avant de modifier le mode.

Remarque Vous ne pouvez pas modifier le mode du contexte actuellement connecté dans ASDM (généralement, le contexte d'administration); consultez Définir le mode du pare-feu (mode unique), à la page 231 pour définir le mode à l'aide de la ligne de commande.

Étape 14 (Facultatif) Pour personnaliser la génération automatique des adresses MAC, consultez Attribuer automatiquement des adresses MAC aux interfaces de contexte, à la page 279.

Étape 15 (Facultatif) Cochez la case **Specify the maximum number of TLS Proxy sessions that the ASA needs to support** (Précisez le nombre maximal de sessions mandataires TLS que l'ASA doit prendre en charge) pour spécifier le nombre maximal de sessions de serveur mandataire TLS pour le périphérique. Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

Attribuer automatiquement des adresses MAC aux interfaces de contexte

Cette section décrit comment configurer la génération automatique des adresses MAC. L'adresse MAC est utilisée pour classer les paquets dans un contexte.

Avant de commencer

- Lorsque vous configurez un nom de pour l'interface dans un contexte, la nouvelle adresse MAC est générée immédiatement. Si vous activez cette fonctionnalité après avoir configuré les interfaces de contexte, les adresses MAC sont générées pour toutes les interfaces immédiatement après leur activation. Si vous désactivez cette fonctionnalité, l'adresse MAC par défaut de chaque interface revient à l'adresse MAC. Par exemple, les sous-interfaces de GigabitEthernet 0/1 utilisent l'adresse MAC de GigabitEthernet 0/1.
- Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC de l'interface dans le contexte.

Procédure

Étape 1 Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

Étape 2 Choisissez **Configuration** > **Context Management** > **Security Contexts** et cochez **Mac-Address auto**. Si vous n'écrivez pas de préfixe, l'ASA génère automatiquement ce dernier en fonction des deux derniers octets.

Étape 3 (Facultatif) Cochez la case **Prefix** (préfixe) et dans le champ, saisissez une valeur décimale entre 0 et 65 535.

Ce préfixe est converti en nombre hexadécimal à quatre chiffres et utilisé dans l'adresse MAC.

Changer entre les contextes et l'espace d'exécution du système

Si vous vous connectez à l'espace d'exécution du système (ou au contexte d'administration), vous pouvez passer d'un contexte à l'autre et effectuer des tâches de configuration et de surveillance dans chaque contexte. La configuration en cours d'exécution que vous modifiez en mode de configuration dépend de votre emplacement. Lorsque vous êtes dans l'espace d'exécution du système, la configuration en cours d'exécution se compose uniquement de la configuration système; lorsque vous êtes dans un contexte, la configuration en cours d'exécution comprend uniquement ce contexte.

Procédure

Étape 1 Dans le panneau Device List (Liste des périphériques), double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif pour configurer le système.

Étape 2 Dans le volet Device List (Liste des périphériques), double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif pour configurer un contexte.

Gérer les contextes de sécurité

Cette section décrit comment gérer les contextes de sécurité.

Supprimer un contexte de sécurité

Vous ne pouvez pas supprimer le contexte d'administration actuel.

Remarque Si vous utilisez le basculement, il y a un délai entre le moment où vous supprimez le contexte sur l'unité active et le moment où le contexte est supprimé de l'unité en veille.

Avant de commencer

Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

Étape 2 Choisissez **Configuration** > **Context Management (Gestion des contextes)** > **Security Contexts (Contextes de sécurité)**.

Étape 3 Sélectionnez le contexte que vous souhaitez supprimer, et cliquez sur **Delete** (Supprimer).

La boîte de dialogue Delete Context (Supprimer un contexte) apparaît.

Étape 4 Si vous souhaitez peut-être rajouter ce contexte ultérieurement et conserver le fichier de configuration pour une utilisation future, décochez la case **Also delete config URL file from the disk** (Supprimer également le fichier d'URL de configuration du disque).

Si vous souhaitez supprimer le fichier de configuration, laissez la case cochée.

Étape 5 Cliquez sur **Yes** (Oui).

Modifier le contexte d'administration

La configuration système n'inclut aucune interface réseau ni aucun paramètre réseau pour elle-même; au contraire, lorsque le système doit accéder à des ressources réseau (comme le téléchargement des contextes à partir du serveur), il utilise l'un des contextes désigné comme contexte d'administration.

Le contexte d'administration est similaire à tout autre contexte, sauf que lorsqu'un utilisateur se connecte au contexte d'administration, cet utilisateur dispose de droits d'administrateur système et peut accéder au système et à tous les autres contextes. Le contexte admin n'est limité en aucune façon et peut être utilisé comme contexte standard. Cependant, comme la connexion au contexte admin vous accorde des privilèges d'administrateur sur tous les contextes, vous devrez peut-être restreindre l'accès au contexte admin aux utilisateurs appropriés.



Remarque Pour ASDM, vous ne pouvez pas modifier le contexte d'administration dans ASDM, car votre session ASDM se déconnecterait. Vous pouvez effectuer cette procédure à l'aide de l'outil d'interface de ligne de commande, en notant que vous devrez vous reconnecter au nouveau contexte d'administration.

Avant de commencer

- Vous pouvez définir n'importe quel contexte comme contexte d'administration, tant que le fichier de configuration est stocké dans la mémoire flash interne.
- Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

Étape 2 Choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

La boîte de dialogue Command Line Interface (Interface de ligne de commande) apparaît.

Étape 3 Entrez la commande suivante :

admin-context *context_name*

Étape 4 Cliquez sur **Send** (envoyer).

Toutes les sessions de gestion à distance, telles que Telnet, SSH ou HTTPS (ASDM), qui sont connectées au contexte d'administration sont terminées. Vous devez vous reconnecter au nouveau contexte d'administration.

Remarque Quelques commandes de configuration système, notamment **ntp server**, identifient un nom d'interface qui appartient au contexte d'administration. Si vous modifiez le contexte d'administration et que le nom de l'interface n'existe pas dans le nouveau contexte d'administration, veillez à mettre à jour toutes les commandes système qui font référence à l'interface.

Modifier l'URL du contexte de sécurité

Cette section décrit comment modifier l'URL du contexte.

Avant de commencer

- Vous ne pouvez pas modifier l'URL du contexte de sécurité sans recharger la configuration à partir de la nouvelle URL. L'ASA fusionne la nouvelle configuration avec la configuration en cours d'exécution.
- La saisie de la même URL fusionne également la configuration enregistrée avec la configuration d'exécution.
- Une fusion ajoute toutes les nouvelles commandes de la nouvelle configuration à la configuration en cours d'exécution.
  - Si les configurations sont identiques, aucune modification ne se produit.
  - Si des commandes sont en conflit ou si des commandes influent sur le fonctionnement du contexte, l'effet de la fusion dépend de la commande. Vous pourriez obtenir des erreurs ou des résultats inattendus. Si la configuration d'exécution est vide (par exemple, si le serveur n'est pas disponible et que la configuration n'a jamais été téléchargée), la nouvelle configuration est utilisée.
- Si vous ne souhaitez pas fusionner les configurations, vous pouvez effacer la configuration d'exécution, ce qui perturbe toute communication en raison du contexte, puis recharger la configuration à partir de la nouvelle URL.
- Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

Étape 2 Choisissez **Configuration** > **Context Management (Gestion des contextes)** > **Security Contexts (Contextes de sécurité)**.

Étape 3 Sélectionnez le contexte que vous souhaitez modifier, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Edit Context (Modifier le contexte) apparaît.

Étape 4 Saisissez une nouvelle URL dans le champ Config URL (Configurer l'URL), puis cliquez sur **OK**.

Le système charge immédiatement le contexte pour qu'il s'exécute.

Recharger un contexte de sécurité

Vous pouvez recharger le contexte de deux manières :

- Effacez la configuration en cours d'exécution, puis importez la configuration de démarrage.

  Cette action efface la plupart des attributs associés au contexte, tels que les connexions et les tables NAT.

- Supprimez le contexte de la configuration système.

  Cette action efface les attributs supplémentaires, tels que l'allocation de mémoire, qui pourraient être utiles pour le dépannage. Cependant, pour rajouter le contexte au système, vous devez redéfinir l'URL et les interfaces.

Recharger en effaçant la configuration

Procédure

Étape 1 Dans le volet Device List (Liste des périphériques), double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

Étape 2 Choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

La boîte de dialogue Command Line Interface (Interface de ligne de commande) apparaît.

Étape 3 Entrez la commande suivante :

clear configure all

Étape 4 Cliquez sur **Send** (envoyer).

La configuration du contexte est effacée.

Étape 5 Choisissez à nouveau **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

La boîte de dialogue Command Line Interface (Interface de ligne de commande) apparaît.

Étape 6 Entrez la commande suivante :

copy startup-config running-config

Étape 7 Cliquez sur **Send** (envoyer).

L'ASA recharge la configuration. L'ASA copie la configuration à partir de l'URL spécifiée dans la configuration système. Vous ne pouvez pas modifier l'URL à partir d'un contexte.

Recharger en supprimant et en rajoutant le contexte

Pour recharger le contexte en le supprimant, puis en le rajoutant, procédez comme suit.

Procédure

Étape 1 Supprimer un contexte de sécurité, à la page 280. Assurez-vous de décocher la case **Also delete config URL file from the disk** (Supprimer également le fichier d'URL de configuration du disque).

Étape 2 Configurer un contexte de sécurité, à la page 276

Supervision des contextes de sécurité

Cette section décrit comment afficher et superviser les renseignements contextuels.

Superviser l'utilisation des ressources de contexte

Procédure

Étape 1 Si vous n'êtes pas déjà en mode système, dans le volet Device List (Liste des périphériques), double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Étape 2 Cliquez sur le bouton **Monitoring** (Supervision) dans la barre d'outils.

Étape 3 Cliquez sur **Context Resource Usage** (Utilisation des ressources de contexte).

Cliquez sur chaque type de ressource pour afficher l'utilisation des ressources pour tous les contextes :

- **ASDM/Telnet/SSH** : affiche l'utilisation des connexions ASDM, Telnet et SSH.
  - Contexte : affiche le nom de chaque contexte.

    Pour chaque méthode d'accès, consultez les statistiques d'utilisation suivantes :
  - Connexions existantes (#) : affiche le nombre de connexions existantes.
  - External Connections (%) (Connexions existantes (%)) : affiche les connexions utilisées par ce contexte en tant que pourcentage du nombre total de connexions utilisées par tous les contextes.
  - Pic de connexions (#) : affiche le pic de connexions depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage**, soit à la suite du redémarrage du périphérique.
- **Routes** : affiche l'utilisation des routes dynamiques.
  - Contexte : affiche le nom de chaque contexte.
  - Connexions existantes (#) : affiche le nombre de connexions existantes.
  - External Connections (%) (Connexions existantes (%)) : affiche les connexions utilisées par ce contexte en tant que pourcentage du nombre total de connexions utilisées par tous les contextes.
  - Pic de connexions (#) : affiche le pic de connexions depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage**, soit à la suite du redémarrage du périphérique.

- **Xlates** : affiche l'utilisation des traductions d'adresses réseau.
  - Contexte : affiche le nom de chaque contexte.
  - Xlates (#) : affiche le nombre de xlates actuels.
  - Xlates (%) : affiche les xlates utilisés par ce contexte en tant que pourcentage du nombre total de xlates utilisés par tous les contextes.
  - Pic (#) : affiche le pic de xlates depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage**, soit à la suite du redémarrage du périphérique.
- **NAT** : affiche le nombre de règles NAT.
  - Contexte : affiche le nom de chaque contexte.
  - NATs (#) : affiche le nombre actuel de règles NAT.
  - NATs (%) : affiche les règles NAT utilisées par ce contexte en tant que pourcentage du nombre total de règles NAT utilisées par tous les contextes.
  - Pic de NAT (#) : affiche le pic de NAT depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage**, soit à la suite du redémarrage du périphérique.
- **Journaux système** : affiche le taux de messages du journal système.
  - Contexte : affiche le nom de chaque contexte.
  - Taux de journal système (#/sec) : affiche le taux actuel de messages du journal du système.
  - Taux de journal système (%) : affiche les messages du journal système générés par ce contexte en pourcentage du nombre total de messages de journal système générés par tous les contextes.
  - (Taux maximum de journal système) : affiche le taux maximum de messages du journal système depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage** , soit en raison du redémarrage du périphérique.
- VPN : affiche l'utilisation des tunnels VPN de site à site.
  - Contexte : affiche le nom de chaque contexte.
  - Connexions VPN : affiche l'utilisation des sessions VPN garanties.
  - Connexions de VPN en rafale : affiche l'utilisation des sessions VPN en rafale.
    - Existant (#) : affiche le nombre de tunnels existants.
    - Pic (#) : affiche le pic de tunnels depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage**, soit à la suite du redémarrage du périphérique.

Étape 4 Cliquez sur **Refresh** (Actualiser) pour actualiser la vue.

Afficher les adresses MAC attribuées

Vous pouvez afficher les adresses MAC générées automatiquement dans la configuration système ou dans le contexte.

Afficher les adresses MAC dans la configuration système

Cette section décrit comment afficher les adresses MAC dans la configuration système.

Avant de commencer

Si vous attribuez manuellement une adresse MAC à une interface, mais que la génération automatique est également activée, l'adresse générée automatiquement continue de s'afficher dans la configuration même si l'adresse MAC manuelle est celle qui est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement s'affichera.

Procédure

Étape 1 Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

Étape 2 Choisissez **Configuration** > **Contexte Management (Gestion de contextes)** > **Security Contextes (Contextes de sécurité)** et affichez les colonnes Primary MAC (MAC principale) et Secondary MAC (MAC secondaire).

Afficher les adresses MAC dans un contexte

Cette section décrit comment afficher les adresses MAC dans un contexte.

Procédure

Étape 1 Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

Étape 2 Choisissez **Configuration** > **Interfaces** et affichez la colonne d'adresses MAC.

Ce tableau affiche l'adresse MAC utilisée; si vous attribuez manuellement une adresse MAC et que la génération automatique est activée, vous ne pouvez afficher que l'adresse générée automatiquement inutilisée à partir de la configuration système.

Historique du mode de contexte multiple

Tableau 15 : Historique du mode de contexte multiple

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Contextes de sécurité multiples	7.0(1)	Le mode de contexte multiple a été introduit. Nous avons introduit les écrans suivants : Configuration > Context Management (Gestion des contextes).
Affectation automatique de l'adresse MAC	7.2(1)	L'affectation automatique de l'adresse MAC aux interfaces de contexte a été introduite. Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité).
Gestion des ressources	7.2(1)	La gestion des ressources a été introduite. Nous avons introduit l'écran suivant : Configuration > Context Management (Gestion des contextes) > Resource Management (Gestion des ressources).
Capteurs virtuels pour IPS	8.0(2)	L'AIP SSM exécutant la version 6.0 et ultérieure du logiciel IPS peut exécuter plusieurs capteurs virtuels, ce qui signifie que vous pouvez configurer plusieurs politiques de sécurité sur l'AIP SSM. Vous pouvez affecter chaque contexte ou ASA en mode unique à un ou plusieurs capteurs virtuels, ou vous pouvez attribuer plusieurs contextes de sécurité au même □capteur virtuel. Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité).
Améliorations de l'affectation automatique de l'adresse MAC	8.0(5)/8.2(2)	Le format de l'adresse MAC a été modifié pour utiliser un préfixe, une valeur initiale fixe (A2) et un schéma différent pour les adresses MAC des unités principale et secondaire dans une paire de basculement. Les adresses MAC sont également conservées de façon permanente pendant les rechargements. L'analyseur de commande vérifie maintenant si la génération automatique est activée; si vous souhaitez également attribuer manuellement une adresse MAC, vous ne pouvez pas commencer l'adresse MAC manuelle par A2. Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité).
Augmentation du nombre maximum de contextes pour les modèles ASA 5550 et 5580	v 8.4(1)	Le nombre maximum de contextes de sécurité pour l'ASA 5550 est passé de 50 à 100. Le nombre maximum pour l'ASA 5580 est passé de 50 à 250.
Affectation automatique de l'adresse MAC activée par défaut	8.5(1)	L'affectation automatique de l'adresse MAC est maintenant activée par défaut. Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité).

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Génération automatique d'un préfixe d'adresse MAC	8.6(1)	En mode de contexte multiple, l'ASA convertit maintenant la configuration de génération automatique de l'adresse MAC en utilisant un préfixe par défaut. L'ASA génère automatiquement ce dernier en fonction des deux derniers octets de l'adresse MAC de l'interface (ASA 5500-X) ou du fond de panier (ASASM). Cette conversion se produit automatiquement lorsque vous rechargez ou si vous réactivez la génération d'adresse MAC. La méthode de génération du préfixe offre de nombreux avantages, notamment une meilleure garantie d'adresses MAC uniques sur un segment. Si vous souhaitez modifier le préfixe, vous pouvez reconfigurer la fonctionnalité avec un préfixe personnalisé. L'ancienne méthode de génération d'adresse MAC n'est plus disponible. **Remarque** Pour maintenir la mise à niveau sans interruption pour les paires de basculement, l'ASA ne convertit *pas* la méthode de génération d'adresse MAC en une configuration existante lors d'un rechargement si le basculement est activé. Cependant, nous vous conseillons fortement de passer manuellement à la méthode de génération du préfixe lorsque vous utilisez le basculement, en particulier pour l'ASASM. Sans la méthode de préfixe, les ASASM installés dans différents numéros de logement subissent un changement d'adresse MAC lors du basculement et peuvent connaître une interruption du trafic. Après la mise à niveau, pour utiliser la méthode de préfixe de génération d'adresse MAC, réactivez la génération d'adresse MAC pour utiliser le préfixe par défaut. Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité)
Affectation automatique de l'adresse MAC désactivée par défaut sur tous les modèles à l'exception de l'ASASM	9.0(1)	L'affectation automatique de l'adresse MAC est maintenant désactivée par défaut, à l'exception de l'ASASM. Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité).
Routage dynamique dans les contextes de sécurité	9.0(1)	Les protocoles de routage dynamique EIGRP et OSPFv2 sont désormais pris en charge en mode de contexte multiple. Les routages OSPFv3, RIP et multidiffusion ne sont pas pris en charge.
Nouveau type de ressource pour les entrées de la table de routage	9.0(1)	Un nouveau type de ressource, les routes, a été créé pour définir le nombre maximum d'entrées de table de routage dans chaque contexte. Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Resource Class (Classe de ressources) > Add Resource Class (Ajouter une classe de ressources)
VPN de site à site en mode de contexte multiple	9.0(1)	Les tunnels VPN de site à site sont désormais pris en charge en mode de contexte multiple.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Nouveau type de ressource pour les tunnels VPN de site à site	9.0(1)	De nouveaux types de ressources (vpn other et vpn burst other) ont été créés pour définir le nombre maximum de tunnels VPN de site à site dans chaque contexte. Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Resource Class (Classe de ressources) > Add Resource Class (Ajouter une classe de ressources)
Nouveau type de ressource pour les négociations de la SA IKEv1	9.1(2)	Un nouveau type de ressource (ikev1 in-negotiation) a été créé pour définir le pourcentage maximum de négociations de la SA IKEv1 dans chaque contexte afin d'éviter de submerger le CPU et les moteurs de chiffrement. Sous certaines conditions (certificats volumineux, vérification des CRL), vous souhaiterez peut-être restreindre cette ressource. Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Resource Class (Classe de ressources) > Add Resource Class (Ajouter une classe de ressources)
Prise en charge du VPN d'accès à distance en mode de contexte multiple	9.5(2)	Vous pouvez désormais utiliser les fonctionnalités d'accès à distance suivantes en mode de contexte multiple : • AnyConnect 3.x ou versions ultérieures (SSL VPN uniquement; pas de prise en charge d'IKEv2) • Configuration centralisée de l'image Secure Client (services client sécurisés) • Mise à niveau de l'image Secure Client (services client sécurisés) • Gestion des ressources de contexte pour les connexions Secure Client (services client sécurisés) **Remarque** La licence Secure Client Premier est requise pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante. Nous avons modifié l'écran suivant : **Configuration** > **Context Management (Gestion des contextes)** > **Resource Class (Classe de ressources)** > **Add Resource Class (Ajouter une classe de ressources)**
Fonction de préremplissage/nom d'utilisateur à partir du certificat pour le mode de contexte multiple	9.6(2)	La prise en charge de SSL Secure Client (services client sécurisés) est étendue, ce qui permet aux interfaces de ligne de commande de la fonctionnalité de préremplissage/nom d'utilisateur à partir du certificat, qui étaient auparavant seulement disponibles en mode unique, d'être également activées en mode de contexte multiple. Nous n'avons pas modifié d'écrans.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Virtualisation flash pour le VPN d'accès à distance	9.6(2)	Le VPN d'accès à distance en mode de contexte multiple prend désormais en charge la virtualisation flash. Chaque contexte peut avoir un espace de stockage privé et un emplacement de stockage partagé en fonction de la mémoire flash totale disponible : • Stockage privé : stockez les fichiers associés uniquement à cet utilisateur et spécifiques au contenu que vous souhaitez pour cet utilisateur. • Stockage partagé : chargez des fichiers dans cet espace et rendez-le accessible à n'importe quel contexte d'utilisateur pour un accès en lecture/écriture une fois que vous l'avez activé. Nous avons modifié les écrans suivants : **Configuration** > **Context Management (Gestion des contextes)** > **Resource Class (Classe de ressources)** > **Add Resource Class (Ajouter une classe de ressources)** **Configuration** > **Context Management (Gestion des contextes)** > **Security Contexts (Contextes de sécurité)**
Profils Secure Client (services client sécurisés) pris en charge dans les périphériques en contexte multiple	9.6(2)	Les profils Secure Client (services client sécurisés) sont pris en charge dans les périphériques en contexte multiple. Pour ajouter un nouveau profil à l'aide d'ASDM, vous devez disposer de la version Secure Client (services client sécurisés) 4.2.00748 ou 4.3.03013 et ultérieure.
Basculement avec état pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple	9.6(2)	Le basculement avec état est maintenant pris en charge pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple. Nous n'avons pas modifié d'écrans.
La politique d'accès dynamique (DAP) du VPN d'accès à distance est prise en charge en mode de contexte multiple	9.6(2)	Vous pouvez maintenant configurer la DAP par contexte en mode de contexte multiple. Nous n'avons pas modifié d'écrans.
Le CoA (changement d'autorisation) du VPN d'accès à distance est pris en charge en mode de contexte multiple	9.6(2)	Vous pouvez maintenant configurer le CoA par contexte en mode de contexte multiple. Nous n'avons pas modifié d'écrans.
La localisation du VPN d'accès à distance est prise en charge en mode de contexte multiple	9.6(2)	La localisation est prise en charge dans le monde entier. Il n'y a qu'un seul ensemble de fichiers de localisation partagés dans différents contextes. Nous n'avons pas modifié d'écrans.
Le VPN d'accès à distance pour IKEv2 est pris en charge en mode de contexte multiple	9.9(2)	Vous pouvez configurer le VPN d'accès à distance en mode de contexte multiple pour IKEv2.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Limitation configurable des sessions d'administration	9.12(1)	Vous pouvez configurer le nombre maximum de sessions administratives agrégées, par utilisateur et par protocole. Auparavant, vous pouviez configurer uniquement le nombre agrégé de sessions. Cette fonctionnalité n'influe pas sur les sessions de console. Notez qu'en mode de contexte multiple, vous ne pouvez pas configurer le nombre de sessions HTTPS, où le maximum est fixé à 5 sessions. La commande **quota management-session** n'est également plus acceptée dans la configuration système et est plutôt disponible dans la configuration du contexte. Le nombre maximum de sessions agrégées est désormais de 15; si vous avez configuré 0 (illimité) ou 16+, lors de la mise à niveau, la valeur passe à 15. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Management Session Quota (Quota de sessions de gestion)**
Le nombre maximum de contextes de Firepower 1140 est passé de 5 à 10	9.16(1)	Le Firepower 1140 prend désormais en charge jusqu'à 10 contextes.



CHAPITRE 10

Basculement pour la haute disponibilité

Ce chapitre décrit comment configurer le basculement actif/en attente ou actif/actif pour une haute disponibilité de l'ASA.

- À propos du basculement, à la page 293
- Licences pour le basculement, à la page 319
- Lignes directrices pour Basculement, à la page 319
- Paramètres par défaut pour le basculement, à la page 323
- Configurer le basculement actif/de secours, à la page 323
- Configurer le basculement actif/actif, à la page 325
- Configurer les paramètres de basculement facultatifs, à la page 326
- Gérer Basculement, à la page 333
- Surveillance de Basculement, à la page 338
- Historique de basculement, à la page 341

À propos du basculement

La configuration du basculement nécessite deux ASA identiques connectés l'un à l'autre par une liaison de basculement dédiée et, éventuellement, un lien d'état. L'intégrité des unités actives et des interfaces est supervisée pour déterminer si elles répondent aux conditions de basculement spécifiques. Si ces conditions sont remplies, le basculement se produit.

Modes de basculement

L'ASA prend en charge deux modes de basculement : le basculement actif/actif et le basculement actif/veille. Chaque mode de basculement a sa propre méthode pour déterminer et effectuer le basculement.

- Dans le basculement actif/veille, un périphérique agit en tant qu'unité active et achemine le trafic. Le deuxième périphérique, désigné comme unité de veille, ne transmet pas activement le trafic. Lors d'un basculement, l'unité active est remplacée par l'unité de veille, qui devient alors active. Vous pouvez utiliser le basculement actif/veille pour les ASA en mode de contexte unique ou multiple.
- Dans une configuration de basculement actif/actif, les deux ASA peuvent transmettre le trafic réseau. Le basculement actif/actif n'est disponible que pour les ASA en mode de contexte multiple. Dans le basculement actif/actif, vous divisez les contextes de sécurité sur l'ASA en 2 *groupes de basculement*. Un groupe de basculement est simplement un groupe logique d'un ou plusieurs contextes de sécurité.

Un groupe est attribué pour être actif sur l'ASA principal, et l'autre groupe est attribué pour être actif sur l'ASA secondaire. Lorsqu'un basculement se produit, il se produit au niveau du groupe de basculement.

Les deux modes de basculement prennent en charge le basculement avec ou sans état.

Configuration système requise Basculement

Les exigences du système Basculement sont des spécifications qui définissent les conditions préalables relatives au matériel, aux logiciels et aux licences nécessaires pour que les Firewall Threat Defensefonctionnent dans une configuration Basculement.

Configuration matérielle requise

Les exigences matérielles sont des spécifications qui garantissent que deux unités dans une configuration Basculement peuvent

- conserver des configurations matérielles identiques, y compris le modèle, les interfaces, les modules et la mémoire vive,
- prendre en charge les fonctionnalités appropriées de synchronisation et de basculement, et
- assurer un fonctionnement fiable en haute accessibilité.

Spécifications relatives aux exigences matérielles

Les deux unités dans une configuration Basculement doivent respecter les exigences suivantes :

- être du même modèle.

  Pour le Firepower 9300, la haute accessibilité est prise en charge uniquement entre des modules de même type. Cependant, les deux châssis peuvent comprendre des modules mixtes. Par exemple, chaque châssis a un SM-56, SM-48 et SM-40. Vous pouvez créer des paires à haute accessibilité entre les modules SM-56, entre les modules SM-48 et entre les modules SM-40.

- Avoir le même nombre et les mêmes types d'interfaces.

  Pour le Firepower 2100 en mode Plateforme et Châssis Firepower 4100/9300 , toutes les interfaces doivent être préconfigurées en FXOS de manière identique avant d'activer Basculement. Si vous modifiez les interfaces après avoir activé Basculement, modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active. Si vous supprimez une interface dans FXOS (p. ex., si vous supprimez un module de réseau, supprimez un canal EtherChannel ou réaffectez une interface à un canal EtherChannel), la configuration ASA conserve les commandes d'origine afin que vous puissiez effectuer les ajustements nécessaires; retirer une interface de la configuration peut avoir des effets considérables. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation ASA.

- Ayez les mêmes modules installés (le cas échéant);
- Ayez la même RAM installée.

Si vous utilisez des unités avec des tailles de mémoire flash différentes dans votre configuration Basculement, assurez-vous que l'unité dotée de la mémoire flash la plus faible dispose de suffisamment d'espace pour contenir les fichiers d'image logicielle et les fichiers de configuration. Si ce n'est pas le cas, la synchronisation

de la configuration de l'unité ayant la plus grande mémoire flash vers l'unité ayant la plus faible mémoire flash échouera.

Exigences relatives au logiciel

Les exigences logicielles sont des spécifications de configuration que les unités Basculement doivent respecter pour fonctionner correctement dans une configuration de basculement.

Spécifications logicielles requises

Les deux unités dans une configuration Basculement doivent respecter les exigences suivantes :

- Être dans le même mode de contexte (simple ou multiple).
- Pour le mode unique : utilisez le même mode de pare-feu (routage ou transparent).

  Dans le mode de contexte multiple, le mode de pare-feu est défini au niveau du contexte et vous pouvez utiliser des modes mixtes.
- Avoir les mêmes version majeure (premier numéro) et mineure (deuxième numéro). Cependant, vous pouvez utiliser temporairement différentes versions du logiciel au cours d'un processus de mise à niveau. Par exemple, vous pouvez mettre à niveau une unité de la version 8.3(1) à la version 8.3(2) et faire en sorte que le basculement reste actif. Nous vous recommandons de mettre à niveau les deux unités à la même version pour assurer la compatibilité à long terme.
- Avoir les mêmes images Secure Client (services client sécurisés). Si les images de la paire de basculement ne concordent pas lors d'une mise à niveau sans interruption, la connexion VPN SSL sans client prend fin à l'étape du redémarrage final du processus de mise à niveau, la base de données affiche une session orpheline et l'ensemble des adresses IP indique que l'adresse IP attribuée au client est « en cours d'utilisation ».
- Être dans le même mode FIPS.
- (Firepower 4100/9300) ont le même mode de déchargement de flux, activé ou désactivé.

Exigences de licence

Il n'est pas nécessaire que les deux unités d'une configuration de basculement aient des licences identiques; les licences se combinent pour créer une licence de grappe de basculement.

Liaisons de basculement et de basculement avec état

Une liaison de basculement et une liaison de basculement avec état sont des connexions dédiées qui

- établissent la communication entre les deux unités dans une configuration de basculement
- nécessitent que la même interface soit utilisée entre les périphériques correspondants pour des raisons de cohérence, et
- transmettent des informations critiques sur le basculement et l'état entre les unités appariées.

Recommandations concernant la configuration

Cisco recommande d'utiliser la même interface entre deux périphériques dans une liaison de basculement ou une liaison de basculement avec état. Par exemple, dans une liaison de basculement, si vous avez utilisé eth0 dans le périphérique 1, utilisez également la même interface (eth0) dans le périphérique 2.



Mise en garde Toutes les informations envoyées sur les liens de basculement et d'état sont envoyées en texte clair, sauf si vous sécurisez la communication avec un tunnel IPsec ou une clé de basculement. Si l'ASA est utilisé pour mettre fin à des tunnels VPN, cette information comprend les noms d'utilisateur, les mots de passe et les clés prépartagées utilisés pour l'établissement des tunnels. La transmission de ces données sensibles en texte clair peut présenter un risque de sécurité important. Nous vous recommandons de sécuriser la communication de basculement avec un tunnel IPsec ou une clé de basculement si vous utilisez l'ASA pour mettre fin aux tunnels VPN.

Liaison de basculement

Les deux unités d'une paire de basculement communiquent en permanence sur une liaison de basculement pour déterminer l'état de fonctionnement de chaque unité.

Données de la liaison de basculement

Les informations suivantes sont transmises par la liaison de basculement :

- L'état de l'unité (actif ou en veille)
- Messages Hello (keep-alives)
- État de la liaison réseau
- Échange d'adresses MAC
- Réplication et synchronisation de la configuration

Interface de la liaison de basculement

Une interface de liaison de basculement est un canal de communication dédié qui

- existe uniquement pour la communication de basculement entre les unités à haute accessibilité
- utilise une interface de données inutilisée (physique, sous-interface, ou EtherChannel)
- ne peut pas être partagée avec les interfaces réseau normales ou le trafic de données d'utilisateur normal, et
- nécessite une taille d'interface spécifique en fonction du modèle du périphérique.

Exigences et restrictions d'interface

Vous pouvez utiliser une interface de données inutilisée (physique, sous-interface ou EtherChannel) comme liaison de basculement; cependant, vous ne pouvez pas spécifier une interface actuellement configurée avec un nom. L'interface de liaison de basculement n'est pas configurée comme une interface réseau normale; il existe pour la communication de basculement uniquement. Cette interface ne peut être utilisée que pour la

liaison de basculement (ainsi que pour le lien d'état). Pour la plupart des modèles, vous ne pouvez pas utiliser une interface de gestion pour le basculement, à moins que cela ne soit explicitement décrit ci-dessous.

L'ASA ne prend pas en charge les interfaces de partage entre les données de l'utilisateur et la liaison de basculement. Vous ne pouvez pas non plus utiliser des sous-interfaces distinctes sur le même parent pour la liaison de basculement et pour les données.

Consultez les consignes suivantes concernant la liaison de basculement :

- 5506-X à 5555-X : vous ne pouvez pas utiliser l'interface de gestion comme liaison de basculement; vous devez utiliser une interface de données. La seule exception est pour le modèle 5506H-X, où vous pouvez utiliser l'interface de gestion comme liaison de basculement.
- 5506H-X : vous *pouvez* utiliser l'interface de gestion Management 1/1 comme liaison de basculement. Si vous le configurez pour le basculement, vous devez recharger le périphérique pour que la modification prenne effet. Dans ce cas, vous ne pouvez pas également utiliser le module ASA Firepower, car il nécessite l'interface de gestion à des fins de gestion.
- Firepower 4100/9300 : vous ne pouvez pas utiliser l'interface de type de gestion pour la liaison de basculement.
- Consultez les lignes directrices suivantes pour dimensionner la liaison.

Tableau 16 : Taille de la liaison de basculement

Modèle	Taille de l'interface pour la liaison combinée de basculement et d'état
Firepower 1010	1 Gbit/sec
Firepower 1100	1 Gbit/sec
Firepower de la série 2100	1 Gbit/sec
Secure Firewall 3100	Secure Firewall 3105, 1 Gbit/s Secure Firewall 3110, 1 Gbit/s Secure Firewall 3120, 1 Gbit/s Secure Firewall 3130, 10 Gbit/s Secure Firewall 3140, 10 Gbit/s
Firepower 4100	10 Gbit/s
Firepower 9300	10 Gbit/s

La fréquence d'alternance est égale au temps de maintien de l'unité (la commande **failover polltime unit**).

Remarque Si vous avez une configuration importante et un temps d'attente d'unité faible, l'alternance entre les interfaces membres peut empêcher l'unité secondaire de se joindre ou de se joindre. Dans ce cas, désactivez l'une des interfaces membres jusqu'à ce que l'unité secondaire se soit jointe.

Pour un EtherChannel utilisé comme liaison de basculement, pour éviter les paquets dans le désordre, une seule interface dans l'EtherChannel est utilisée. Si cette interface échoue, l'interface suivante de l'EtherChannel est utilisée. Vous ne pouvez pas modifier la configuration de l'EtherChannel lorsqu'il est utilisé comme liaison de basculement.

Connexion de la liaison de basculement

La liaison de basculement permet la communication et la coordination entre les unités dans une configuration de basculement.

Vous devez établir une connexion physique entre les unités de basculement pour activer une fonctionnalité de basculement appropriée.

Procédure

Connectez la liaison de basculement de l'une des deux manières suivantes :

- À l'aide d'un commutateur, sans autre périphérique sur le même segment de réseau (domaine de diffusion ou VLAN) que les interfaces de basculement de l' ASA Firewall Threat Defense.
- L'utilisation d'un câble Ethernet pour connecter les unités directement, sans avoir besoin d'un commutateur externe.

Si vous n'utilisez pas de commutateur entre les unités, et en cas de défaillance de l'interface, la liaison est interrompue sur les deux homologues. Cette condition peut nuire aux efforts de dépannage, car vous ne pouvez pas facilement déterminer quelle unité a l'interface défaillante qui a entraîné la défaillance du lien.

L'ASA Firewall Threat Defense prend en charge Auto-MDI/MDIX sur ses ports Ethernet en cuivre, vous pouvez donc utiliser un câble croisé ou droit. Si vous utilisez un câble droit, l'interface détecte automatiquement le câble et échange l'une des paires de transmission/réception contre MDIX.

La liaison de basculement est connectée physiquement et prête à être configurée.

Liaisons de basculement dynamique

Une liaison de basculement dynamique est une connexion réseau qui

- transmet les informations sur l'état de connexion entre les unités de basculement, et
- doit être configurée pour activer la fonctionnalité de basculement dynamique.

Exigences de configuration de la liaison de basculement dynamique

Pour utiliser le basculement avec état, vous devez configurer une liaison de basculement avec état (également appelé lien d'état) pour transmettre les informations sur l'état de la connexion.

Liaisons de basculement partagées

Une liaison de basculement partagée est une méthode permettant d'économiser des interfaces et à plusieurs fonctions réseau d'utiliser la même connexion de basculement; il convient toutefois d'envisager des interfaces dédiées pour les liaisons d'état et de basculement dans les configurations de grande taille et les réseaux à trafic élevé.

Interface dédiée

Une interface dédiée est une configuration d'interface de données qui utilise une interface physique dédiée ou EtherChannel spécifiquement pour la liaison d'état dans les déploiements de basculement.

Considérations sur la performance

Vous pouvez utiliser une interface de données dédiée—physique ou EtherChannel—pour la liaison d'état. Pour les exigences relatives à un lien d'état dédié, consultez Interface de la liaison de basculement, à la page 296. Consultez la section sur la connexion de la liaison d'état pour obtenir des renseignements supplémentaires Connexion de la liaison de basculement, à la page 298.

Pour des performances optimales lors de l'utilisation du basculement longue distance, la latence de la liaison d'état doit être inférieure à 10 millisecondes et non supérieure à 250 millisecondes. Si la latence est supérieure à 10 millisecondes, une certaine dégradation des performances se produit en raison de la retransmission des messages de basculement.

Éviter le basculement interrompu et les liaisons de données

Nous recommandons que les liens de basculement et les interfaces de données empruntent différentes voies pour réduire le risque d'échec de toutes les interfaces en même temps. Si la liaison de basculement est hors service, l'ASA peut utiliser les interfaces de données pour déterminer si un basculement est requis. Ensuite, l'opération de basculement est suspendue jusqu'à ce que l'intégrité de la liaison de basculement soit restaurée.

Consultez les scénarios de connexion suivants pour concevoir un réseau de basculement résilient.

Scénario 1 (non recommandé)

Si un seul commutateur ou un ensemble de commutateurs est utilisé pour connecter les interfaces de basculement et de données entre deux ASA, quand un commutateur ou une liaison inter-commutateurs sont en panne, les deux ASA deviennent actifs. Par conséquent, les deux méthodes de connexion illustrées dans les figures suivantes ne sont PAS conseillées.

Illustration 49 : Connexion avec un commutateur unique : non recommandée

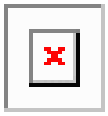
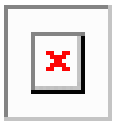


Illustration 50 : Connexion avec un double commutateur : non recommandée



Scénario 2 (recommandé)

Nous conseillons que les liaisons de basculement n'utilisent PAS le même commutateur que les interfaces de données. Au lieu de cela, utilisez un commutateur différent ou utilisez un câble direct pour connecter la liaison de basculement, comme le montrent les figures suivantes.

Illustration 51 : Connexion avec un autre commutateur

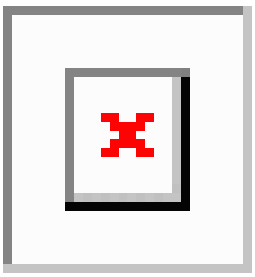
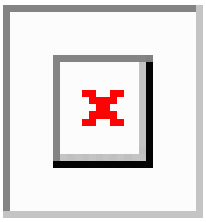


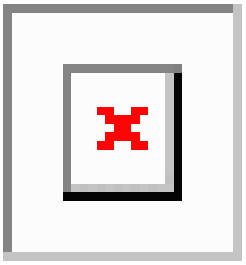
Illustration 52 : Connexion avec un câble



Scénario 3 (recommandé)

Si les interfaces de données ASA sont connectées à plusieurs ensembles de commutateurs, une liaison de basculement peut être connecté à l'un des commutateurs, de préférence le commutateur du côté sécurisé (interne) du réseau, comme le montre la figure suivante.

Illustration 53 : Connexion avec un commutateur sécurisé



Les adresses MAC et les adresses IP en Basculement

Les adresses MAC et les adresses IP dans Basculement sont des mécanismes d'adressage réseau qui

- fournissent une identification unique des interfaces réseau pendant les scénarios de basculement
- maintiennent la connectivité réseau lorsque les périphériques principaux deviennent indisponibles, et
- assurent un flux de trafic transparent entre les configurations actives et en veille.

Types de configuration d'adresses

Lorsque vous configurez vos interfaces, vous pouvez spécifier une adresse IP active et une adresse IP de secours sur le même réseau. En général, lors d'un basculement, la nouvelle unité active prend en charge les

adresses IP et MAC actives. Étant donné que les périphériques réseau ne constatent aucun changement dans l'association d'adresses MAC à l'adresse IP, aucune entrée ARP ne change et n'expire sur le réseau.



Remarque Bien que recommandée, l'adresse de secours n'est pas obligatoire. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien. Vous ne pouvez pas non plus vous connecter à l'unité de secours sur cette interface à des fins de gestion.

L'adresse IP et l'adresse MAC du lien d'état ne changent pas lors du basculement.

Les configurations actives/en veille utilisent des méthodes de traitement des adresses spécifiques :

Pour le Basculement (actif/veille), consultez les documents suivants pour connaître l'utilisation de l'adresse IP et de l'adresse MAC lors d'un événement de basculement :

1. L'unité active utilise toujours les adresses IP et MAC de l'unité principale.
2. Lorsque l'unité active bascule, l'unité en veille adopte les adresses IP et MAC de l'unité défaillante et commence à transmettre le trafic.
3. Lorsque l'unité défaillante est remise en ligne, elle est maintenant en état de veille et prend le relais des adresses IP et MAC de secours.

Toutefois, si l'unité secondaire démarre sans détecter l'unité principale, l'unité secondaire devient l'unité active et utilise ses propres adresses MAC, car elle ne connaît pas les adresses MAC de l'unité principale. Lorsque l'unité principale devient disponible, les adresses MAC de l'unité secondaire (active) changent pour celles de l'unité principale, ce qui peut entraîner une interruption de votre trafic réseau. De même, si vous remplacez l'unité principale par un nouveau matériel, une nouvelle adresse MAC est utilisée.

Si vous désactivez le basculement et définissez les configurations de basculement à un état désactivé, vous devrez reprendre manuellement le basculement ou redémarrer le périphérique. Il est conseillé d'utiliser la commande **failover reset** et de reprendre le basculement au lieu de redémarrer le périphérique. Si vous rechargez l'unité de secours avec la configuration de basculement désactivée, l'unité de secours démarre en tant qu'unité active et utilise les adresses IP et MAC de l'unité principale. Cela conduit à des adresses IP en double et entraîne des perturbations du trafic réseau. Utilisez la commande **failover reset** pour activer le basculement et restaurer le flux de trafic.



Remarque Si vous activez le basculement sur un périphérique autonome, les interfaces de données tombent en panne lors de la négociation du basculement, interrompant le trafic.

Les adresses MAC virtuelles empêchent cette perturbation, car les adresses MAC actives sont connues de l'unité secondaire au démarrage et restent les mêmes dans le cas du nouveau matériel de l'unité principale. Nous vous recommandons de configurer l'adresse MAC virtuelle sur les unités principale et secondaire pour vous assurer que l'unité secondaire utilise les adresses MAC correctes lorsqu'il s'agit de l'unité active, même si elle est mise en ligne avant l'unité principale. Si vous ne configurez pas d'adresses MAC virtuelles, vous devrez peut-être effacer les tableaux ARP sur les routeurs connectés pour restaurer le flux de trafic. ASA n'envoie pas d'ARP gratuits pour les adresses NAT statiques lorsque l'adresse MAC change, de sorte que les routeurs connectés n'apprennent pas le changement d'adresse MAC pour ces adresses.

Pour le basculement actif, consultez les documents suivants pour connaître l'utilisation de l'adresse IP et de l'adresse MAC lors d'un événement de basculement :

1. L'unité principale génère automatiquement des adresses MAC actives et de secours pour toutes les interfaces dans les contextes des groupes de basculement 1 et 2. Vous pouvez également configurer manuellement les adresses MAC au besoin, par exemple en cas de conflit d'adresses MAC.
2. Chaque unité utilise les adresses IP et MAC actives pour son groupe de basculement actif et les adresses de secours pour son groupe de basculement en veille. Par exemple, l'unité principale est active pour le groupe de basculement 1, elle utilise donc les adresses actives pour les contextes du groupe de basculement 1. Elle est en veille pour les contextes du groupe de basculement 2, où elle utilise les adresses de secours.
3. Lors du basculement d'une unité, l'autre unité prend les adresses IP et les adresses MAC actives du groupe de basculement et commence à transmettre le trafic.
4. Lorsque l'unité défaillante est remise en ligne et que vous avez activé l'option de préemption, elle reprend le groupe de basculement.

Les configurations actives/actives mettent en œuvre une gestion supplémentaire des adresses :

Les adresses MAC virtuelles fournissent des fonctionnalités spécialisées :

L'ASA comporte plusieurs méthodes pour configurer les adresses MAC virtuelles. Nous vous recommandons d'utiliser une seule méthode. Si vous définissez l'adresse MAC à l'aide de plusieurs méthodes, l'adresse MAC utilisée dépend de nombreuses variables et peut ne pas être prédictible. Les méthodes manuelles comprennent la commande interface mode **mac-address**, la commande **failover mac address** et, pour le basculement actif/actif, la commande failover group mode **mac address**, en plus des méthodes de génération automatique décrites ci-dessous.

En mode de contexte multiple, vous pouvez configurer l'ASA pour générer automatiquement des adresses MAC virtuelles actives et de secours pour les interfaces partagées, et ces affectations sont synchronisées avec l'unité secondaire (voir la commande **mac-address auto**). Pour les interfaces non partagées, vous pouvez définir manuellement les adresses MAC pour le mode actif/veille (le mode actif/actif génère automatiquement les adresses MAC pour toutes les interfaces).

Pour le basculement actif, les adresses MAC virtuelles sont toujours utilisées, avec des valeurs par défaut ou des valeurs que vous pouvez définir par interface.

Les mises à jour du tableau d'adresses MAC se produisent lors des événements de basculement :

Pendant le basculement, le périphérique désigné comme le nouveau périphérique actif génère des paquets de multidiffusion pour chaque entrée d'adresse MAC dans le tableau MAC et les envoie à toutes les interfaces du groupe de ponts. Cette action incite les commutateurs en amont du groupe de ponts à mettre à jour leurs tables de routage avec l'interface du nouveau périphérique actif pour assurer un transfert précis du trafic.

Le temps nécessaire pour générer des paquets de multidiffusion et mettre à jour les tables de routage des commutateurs en amont dépend du nombre d'entrées dans le tableau d'adresses MAC et du nombre d'interfaces du groupe de ponts. Utilisez la commande **show failover statistics state-switch-delay** pour afficher les statistiques relatives aux retards rencontrés lors des événements de basculement.

Basculement avec et sans état

L'ASA prend en charge deux types de basculement, sans état et avec état, pour les modes actif/veille et actif/actif.

Remarque Certains éléments de configuration pour le SSL VPN sans client (comme les signets et la personnalisation) utilisent le sous-système de basculement VPN, qui fait partie du basculement dynamique. Vous devez utiliser le basculement dynamique pour synchroniser ces éléments entre les membres de la paire de basculement. Le basculement sans état n'est pas conseillé pour le SSL VPN sans client.

Basculement sans état

Lorsqu'un basculement se produit, toutes les connexions actives sont abandonnées. Les clients doivent rétablir les connexions lorsque la nouvelle unité active prend le relais.

Remarque Certains éléments de configuration pour le SSL VPN sans client (comme les signets et la personnalisation) utilisent le sous-système de basculement VPN, qui fait partie du basculement dynamique. Vous devez utiliser le basculement dynamique pour synchroniser ces éléments entre les membres de la paire de basculement. Le basculement sans état (standard) n'est pas conseillé pour le SSL VPN sans client.

Basculement avec état

Un basculement avec état est un mécanisme de haute accessibilité qui

- transmet sans interruption les informations d'état par connexion de l'unité active à l'unité de secours
- conserve les informations de connexion après un basculement, et
- permet aux applications d'utilisateur final prises en charge de poursuivre les sessions de communication sans se reconnecter.

Opération de basculement avec état

Lorsque le basculement dynamique est activé , l'unité active transmet en permanence des informations sur l'état de la connexion à l'unité en veille, ou en cas de basculement actif/actif, entre les groupes de basculement actif et de secours. Après un basculement, les mêmes informations de connexion sont disponibles sur la nouvelle unité active. Les applications de l'utilisateur final prises en charge ne sont pas tenues de se reconnecter pour conserver la même session de communication.

Fonctionnalités prises en charge

Les fonctionnalités prises en charge sont des fonctionnalités de haute accessibilité qui

- permettent la transmission des renseignements d'état au périphérique ASA en veille pendant le basculement avec état
- maintiennent les états de connexion et les renseignements essentiels pour un flux de trafic transparent, et
- garantissent un minimum de perturbations lors des événements de basculement.

Types de renseignements d'état

Pour le basculement avec état, les renseignements d'état suivants sont transmis au périphérique en veille :

- table de traduction NAT
- Les connexions et les états TCP et UDP. Les autres types de protocoles IP et ICMP ne sont pas analysés par l'unité active, car ils sont établis sur la nouvelle unité active à l'arrivée d'un nouveau paquet.
- Le tableau de connexion HTTP (sauf si vous activez la duplication HTTP).
- Les états de la connexion HTTP (si la duplication HTTP est activée) : Par défaut, l'ASA ne reproduit pas les informations de session HTTP lorsque le basculement avec état est activé. Nous vous suggérons d'activer la duplication HTTP.
- Les états de la connexion SCTP sont inclus. Le basculement avec état de l'inspection SCTP est effectué au mieux. Pendant le basculement, si des paquets SACK sont perdus, la nouvelle unité active abandonnera tous les autres paquets dans le désordre dans la file d'attente jusqu'à ce que le paquet manquant soit reçu.
- La table ARP
- La table des ponts de couche 2 (pour les groupes de ponts)
- La table ISAKMP et IPsec SA
- La base de données sur les connexions GTP-PDP
- Sessions de signalisation SIP et trous d'épingle.
- ICMP connection state (état de connexion ICMP) : la duplication de connexion ICMP n'est activée que si l'interface respective est affectée à un groupe de routage dissymétrique.
- Tables de routage statiques et dynamiques : le basculement dynamique participe aux protocoles de routage dynamiques, tels que OSPF et EIGRP, de sorte que les itinéraires appris par les protocoles de routage dynamiques sur l'unité active sont conservés dans une table RIB (Routing Information Base) sur l'unité en attente. Lors d'un basculement, les paquets se déplacent normalement avec une perturbation minimale du trafic, car l'unité secondaire active est initialement soumise à des règles qui reflètent l'unité principale. Immédiatement après le basculement, le délai de reconvergence démarre sur l'unité nouvellement active. Ensuite, le numéro de la période pour la table RIB est incrémenté. Pendant la reconvergence, les routes OSPF et EIGRP sont mises à jour avec un nouveau numéro de période. Une fois la minuterie expirée, les entrées de route périmées (déterminées par le numéro de période) sont supprimées du tableau. Le RIB contient ensuite les informations de transfert les plus récentes du protocole de routage sur la nouvelle unité active.



Remarque Les routages ne sont synchronisés que pour les événements de connexion ou de déconnexion sur une unité active. Si le lien est actif ou inactif sur l'unité de secours, les routages dynamiques envoyés à partir de l'unité active peuvent être perdus. Ce comportement est tout à fait normal et attendu.

- Serveur DHCP : les baux d'adresses DHCP ne sont pas répliqués. Cependant, un serveur DHCP configuré sur une interface enverra un message ping pour s'assurer qu'une adresse n'est pas utilisée avant d'accorder l'adresse à un client DHCP, donc il n'y a pas d'incidence sur le service. Les informations d'état ne sont pas pertinentes pour le relais DHCP ou DDNS.

- Sessions Cisco IPSoftPhone : Si un basculement se produit pendant une session Cisco IPSoftPhone active, l'appel reste actif, car les informations sur l'état de la session d'appel sont répliquées sur l'unité de secours. Lorsque l'appel est terminé, le client IPSoftPhone perd la connexion avec Cisco Call Manager. Cette perte de connexion se produit parce qu'il n'y a pas d'informations de session pour le message de raccrochage CTIQBE sur l'unité de secours. Lorsque le client IP SoftPhone ne reçoit pas de réponse du gestionnaire d'appels dans un certain délai, il considère que le gestionnaire d'appels est injoignable et se désenregistre.
- VPN d'accès à distance : les utilisateurs finaux du VPN d'accès à distance n'ont pas à s'authentifier ou à reconnecter la session VPN après un basculement. Cependant, les applications fonctionnant sur la connexion VPN pourraient perdre des paquets pendant le processus de basculement et ne pas se rétablir après la perte de paquets.
- De toutes les connexions, seules celles établies seront répliquées sur le périphérique de secours.

Fonctionnalités non prises en charge

Les fonctionnalités non prises en charge sont les capacités du périphérique qui

- ne sont pas transmises à l'unité de secours ASA dans le basculement dynamique
- ne conservent pas les informations d'état pendant les événements de basculement, et
- peuvent nécessiter un rétablissement après un basculement.

Limites des informations d'état

Pour le basculement avec état, les informations d'état suivantes ne sont pas transmises à l'ASA de secours :

- Le tableau d'authentification des utilisateurs (uauth)
- Le routage de multidiffusion

Exigences en matière de groupes de ponts pour le basculement

Il y a des considérations particulières à prendre en matière de basculement lors de l'utilisation de groupes de ponts.

Exigences en matière de groupes de ponts pour les appareils, ASAv

Lorsque l'unité active bascule sur l'unité en veille, le port du commutateur connecté exécutant le protocole Spanning Tree (STP) peut passer dans un état bloquant pendant 30 à 50 secondes lorsqu'il détecte le changement de topologie. Pour éviter les pertes de trafic lorsque le port est dans un état bloquant, vous pouvez configurer l'une des solutions de contournement suivantes en fonction du mode du port du commutateur :

- Mode d'accès : activez la fonctionnalité STP PortFast sur le commutateur :

```
interface interface_id
  spanning-tree portfast
```

La fonctionnalité PortFast fait immédiatement passer le port en mode de transfert STP lors de l'établissement de la liaison. Le port participe toujours à STP. Ainsi, si le port doit faire partie de la boucle, le port finit par passer en mode de blocage STP.

- Mode de liaison : bloquez les BPDU sur l'ASA sur les interfaces membres d'un groupe de ponts avec un critère d'accès EtherType.

```
access-list id ethertype deny bpdu
access-group id in interface name1
access-group id in interface name2
```

Le blocage des BPDU désactive le STP sur le commutateur. Assurez-vous de ne pas avoir de boucles concernant l'ASA dans la disposition de votre réseau.

Si aucune des options ci-dessus n'est possible, vous pouvez utiliser l'une des solutions de contournement moins souhaitables suivantes qui a une incidence sur la fonctionnalité de basculement ou la stabilité STP :

- Désactivez la supervision d'interface.
- Augmentez le temps de rétention à une valeur élevée qui permettra au STP de converger avant le basculement des ASA.
- Réduisez les minuteries STP pour permettre au STP de converger plus rapidement que le temps de rétention de l'interface.

Supervision de l'intégrité du basculement

La supervision de l'intégrité du basculement est une fonctionnalité du système qui supervise l'intégrité globale et l'intégrité des interfaces de chaque unité.

Tests de supervision de l'intégrité

L' ASA Firewall Threat Defense effectue les tests pour déterminer l'état de chaque unité. Cette section comprend des informations sur la façon dont l'ASA effectue les tests pour déterminer l'état de chaque unité.

Surveillance de l'intégrité de l'unité

La surveillance de l'intégrité de l'unité est un mécanisme de basculement qui

- détermine l'intégrité des unités homologues en surveillant la liaison de basculement à l'aide de messages Hello,
- envoie des messages LANTEST sur chaque interface de données lorsque trois messages Hello consécutifs ne sont pas reçus, et
- initie les actions de basculement appropriées en fonction de la réactivité de l'unité homologue.

Comportement de la surveillance de l'intégrité de l'unité

L'ASA détermine l'intégrité de l'autre unité en surveillant la liaison de basculement à l'aide de messages Hello. Lorsqu'une unité ne reçoit pas trois messages Hello consécutifs sur la liaison de basculement, l'unité envoie des messages LANTEST sur chaque interface de données, y compris la liaison de basculement, pour valider si l'homologue réagit ou non. Pour les périphériques Firepower 9300 et 4100, vous pouvez activer la surveillance de la détection de transfert bidirectionnel (BFD), qui est plus fiable que les messages Hello. L'action de l'ASA dépend de la réponse de l'autre unité. Voici les actions possibles :

- Si l'ASA reçoit une réponse sur la liaison de basculement, il ne bascule pas.

- Si l'ASA ne reçoit pas de réponse sur la liaison de basculement, mais qu'il reçoit une réponse sur une interface de données, l'unité ne bascule pas. La liaison de basculement est marqué comme ayant échoué. Vous devez restaurer la liaison de basculement dès que possible, car l'unité ne peut pas basculer sur l'unité de secours lorsque la liaison de basculement est inactif.
- Si l'ASA ne reçoit de réponse sur aucune interface, l'unité en veille passe en mode actif et classe l'autre unité comme en panne.

Supervision des interfaces

La supervision des interfaces est une fonctionnalité de basculement qui

- surveille l'intégrité d'un maximum de 1 025 interfaces afin de détecter les défaillances d'interface,
- effectue des tests d'interface lorsque les messages Hello ne sont pas reçus dans les 15 secondes, et
- déclenche le basculement lorsque le nombre d'interfaces défaillantes atteint le seuil défini.

Fonctionnement de la supervision des interfaces

Vous pouvez surveiller jusqu'à 1 025 interfaces (en mode contextes multiples, réparties entre tous les contextes). Vous devez surveiller les interfaces importantes. Par exemple, en mode de contexte multiple, vous pouvez configurer un contexte pour surveiller une interface partagée : comme l'interface est partagée, tous les contextes bénéficient de la surveillance.

Lorsqu'une unité ne reçoit pas de messages Hello sur une interface surveillée pendant 15 secondes (valeur par défaut), elle exécute des tests d'interface. (Pour modifier la période, consultez **Configuration** > **Device Management** > **High Availability and Scalability** > **Failover** > **Criteria** > **Failover Poll Times**. (Configuration > Gestion du périphérique > Haute disponibilité et évolutivité > Basculement > Critères > Durées d'interrogation du basculement).) Si l'un des tests d'interface échoue pour une interface, mais que cette même interface sur l'autre unité continue de transmettre le trafic avec succès, l'interface est considérée comme ayant échoué et leASA arrête d'exécuter les tests.

Si le seuil que vous avez défini pour le nombre d'interfaces défaillantes est atteint (voir **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute accessibilité et évolutivité)** > **Failover** > **Criteria (Critères de basculement)** > **Interface Policy (Politique d'interface)**), et que l'unité active comporte plus d'interfaces défaillantes que l'unité en attente, un basculement se produit. Si une interface échoue sur les deux unités, les deux interfaces passent à l'état « Inconnu » et ne sont pas prises en compte dans la limite de basculement définie par la politique d'interface de basculement.

Une interface devient de nouveau opérationnelle si elle reçoit du trafic. Un ASA défaillant passe en mode veille si le seuil de défaillance de l'interface n'est plus atteint.

Si une interface a des adresses IPv4 et IPv6 configurées, l'ASA utilise les adresses IPv4 pour effectuer la surveillance de l'intégrité. Si une interface n'a que des adresses IPv6 configurées, l'ASA utilise la découverte des voisins IPv6 au lieu d'ARP pour effectuer les tests de surveillance de l'intégrité. Pour le test de ping de diffusion, l'ASA utilise l'adresse de tous les nœuds IPv6 (FE02::1).



Remarque Si une unité défaillante ne récupère pas et que vous pensez qu'elle ne devrait pas tomber en panne, vous pouvez réinitialiser l'état en saisissant la commande « **failover reset** ». Si la condition de basculement persiste, l'unité échouera à nouveau.

Tests d'interface

Les tests d'interface sont des mécanismes de supervision qui :

- évaluent l'état opérationnel de l'interface pendant les scénarios de basculement
- s'exécutent séquentiellement pendant environ 1,5 seconde par test par défaut, ou pendant 1/16 du temps d'attente de l'interface de basculement (voir **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute accessibilité et évolutivité)** > **Failover (Basculement)** > **Criteria (Critères)** > **Failover Poll Times (Temps d'interrogation du basculement)**), et
- déterminent l'état de défaillance de l'interface sur les unités du périphérique ASA.

Séquence de test d'interface

Le périphérique ASA utilise ces tests d'interface dans l'ordre :

1. Test de liaison (Active/En panne) : test de l'état de l'interface. Si le test de liaison active/désactivée indique que l'interface est en panne, l'ASA la considère comme ayant échoué et les tests s'arrêtent. Si l'état est Activé, l'ASA effectue le test d'activité réseau.
2. Test d'activité réseau : test d'activité réseau reçu. Au début du test, chaque unité efface son nombre de paquets reçus pour ses interfaces. Dès qu'une unité reçoit des paquets admissibles pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, l'ASA démarre le test ARP.
3. Test ARP : Un test des réponses ARP réussies. Chaque unité envoie une seule requête ARP pour l'adresse IP dans l'entrée la plus récente de son tableau ARP. Si l'unité reçoit une réponse ARP ou un autre trafic réseau pendant le test, l'interface est considérée comme opérationnelle. Si l'unité ne reçoit pas de réponse ARP, l'ASA envoie une seule requête ARP pour l'adresse IP dans l'entrée *suivante* du tableau ARP. Si l'unité reçoit une réponse ARP ou un autre trafic réseau pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, l'ASA démarre le test ping de diffusion.
4. Test de ping de diffusion : un test de réponses au ping réussies. Chaque unité envoie un message Ping de diffusion, puis compte tous les paquets reçus. Si l'unité reçoit des paquets pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, les tests recommencent avec le test ARP. Si les deux unités continuent de ne recevoir aucun trafic venant des tests ARP et de ping de diffusion, ces tests continueront à se dérouler à l'infini.

État de l'interface

L'état de l'interface est un indicateur de supervision qui

- affiche l'état opérationnel actuel des interfaces supervisées dans une configuration de basculement
- suit la réception du trafic et la communication de paquets Hello entre les unités homologues, et
- détermine si une interface est supervisée activement par le processus de basculement.

Types d'état d'interface

Les interfaces supervisées peuvent avoir les types d'état suivants :

- **Unknown** (Inconnu) : état initial. Cet état peut également signifier qu'il ne peut pas être déterminé.
- **Normal** : l'interface reçoit du trafic.
- **Testing** (En test) : les messages Hello ne sont pas entendus sur l'interface pendant cinq cycles d'interrogation.
- **Link Down** (Liaison en panne) : l'interface ou le VLAN est administrativement inactif.
- **No Link** (Aucune liaison) : la liaison physique de l'interface est inactive.
- **Failed** (Échec) : aucun trafic n'est reçu sur l'interface, mais du trafic est détecté sur l'interface homologue.

et seuils de délai de détection

les seuils de délai de détection sont des mécanismes de haute accessibilité qui :

- lancent le basculement automatique lorsque des conditions de défaillance spécifiques se produisent sur l'unité active,
- supervisent l'intégrité du système au moyen de seuils de détection et de paramètres de délai configurables, et
- assurent la continuité du service en transférant le contrôle à l'unité de secours lorsque les défaillances dépassent les limites définies.

Événements déclencheurs de basculement et paramètres de délai

Les événements suivants déclenchent le basculement dans une paire à haute accessibilité Firepower :

- Plus de 50 % des instances Snort sur l'unité active sont en panne.
- L'espace disque de l'unité active est plein à plus de 90 %.
- La commande **no failover active** est exécutée sur l'unité active ou la commande **failover active** est exécutée sur l'unité de secours.
- L'unité active comporte plus d'interfaces défaillantes que l'unité en veille.
- La défaillance d'interface sur le périphérique actif dépasse le seuil configuré.

  Par défaut, la défaillance d'une seule interface entraîne le basculement. Vous pouvez modifier la valeur par défaut en configurant un seuil pour le nombre d'interfaces ou un pourcentage d'interfaces surveillées qui doivent échouer pour que le basculement se produise. Si le seuil est dépassé sur le périphérique actif, le basculement se produit. Si le seuil est dépassé sur le périphérique de secours, l'unité passe à l'état **Fail** (Échec).

  Pour modifier les critères de basculement par défaut, saisissez la commande suivante en mode de configuration globale :

Tableau 17 : Commande de stratégie d'interface

Commande	Objectif
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	Modifie les critères de basculement par défaut. Lorsque vous spécifiez un nombre spécifique d'interfaces, l'argument *num* peut être compris entre 1 et 250. Lors de la spécification d'un pourcentage d'interfaces, l'argument *num* peut être compris entre 1 et 100.



Remarque Si vous basculez manuellement à l'aide de l'interface de ligne de commande ou de l'ASDM, ou si vous rechargez l'ASA, le basculement démarre immédiatement et n'est pas soumis aux minuteurs ci-dessous.

Tableau 18 :

Condition/	Minimum	Par défaut	Maximum
L'unité active n'est plus alimentée, le matériel tombe en panne, le logiciel est rechargé ou se bloque. Lorsque l'un de ces événements se produit, les interfaces surveillées ou la liaison de basculement ne reçoivent aucun message Hello.	800 milliseconde	15 secondes	45 secondes
Lien de l'interface de la carte principale de l' unité active en panne.	500 millisecondes	5 secondes	15 secondes
Lien d'interface de module 4GE de l'unité active inactif.	2 secondes	5 secondes	15 secondes
L'interface de l'unité active est active, mais un problème de connexion entraîne des tests d'interface.	5 secondes	25 secondes	75 secondes

Synchronisation de la configuration

Le basculement comprend différents types de synchronisation de configuration.

Réplication de la configuration en cours d'exécution

La réplication de la configuration en cours d'exécution se produit lorsque l'un des périphériques de la paire de basculement ou les deux démarrent.

Dans le basculement actif/veille, les configurations sont toujours synchronisées de l'unité active avec l'unité en veille.

Dans le basculement actif/actif, quelle que soit l'unité de démarrage, elle obtient la configuration en cours d'exécution de l'unité qui démarre en premier, quelle que soit la désignation principale ou secondaire de l'unité de démarrage. Une fois que les deux unités sont opérationnelles, les commandes saisies dans l'espace

d'exécution du système sont répliquées à partir de l'unité sur laquelle le groupe de basculement 1 est à l'état actif.

Lorsque l'unité de secours/seconde termine son démarrage initial, elle efface sa configuration en cours d'exécution (à l'exception des commandes **failover** nécessaires pour communiquer avec l'unité active) et l'unité active envoie sa configuration complète à l'unité de secours/seconde. Lorsque la réplication démarre, la console ASA sur l'unité active affiche le message « Début de la réplication de la configuration : envoi à l'unité jumelle » et lorsqu'elle est terminée, l'ASA affiche le message « Fin de la réplication de la configuration vers l'unité jumelle ». Selon la taille de la configuration, la réplication peut prendre de quelques secondes à plusieurs minutes.

Sur l'unité recevant la configuration, la configuration existe uniquement dans la mémoire en cours d'exécution. Vous devez enregistrer la configuration dans la mémoire flash. Par exemple, dans le basculement actif/actif, saisissez la commande **write memory all** dans l'espace d'exécution du système sur l'unité qui a le groupe de basculement 1 à l'état actif. La commande est répliquée sur l'unité homologue, qui continue d'écrire sa configuration dans la mémoire flash.



Remarque Pendant la réplication, les commandes saisies sur l'unité qui envoie la configuration peuvent ne pas être répliquées correctement sur l'unité homologue, et les commandes saisies sur l'unité qui reçoit la configuration peuvent être remplacées par la configuration en cours de réception. Évitez de saisir des commandes sur l'une ou l'autre des unités de la paire de basculement pendant le processus de réplication de la configuration.

Réplication du fichier

La synchronisation de la configuration ne réplique pas les fichiers et composants de configuration suivants. Vous devez donc copier ces fichiers manuellement pour qu'ils correspondent :

- Images Secure Client (services client sécurisés)
- Images CSD
- Profils Secure Client (services client sécurisés)

  L'ASA utilise un fichier mis en mémoire cache pour le profil Secure Client (services client sécurisés) stocké dans cache:/stc/profiles, et non le fichier stocké dans le système de fichiers flash. Pour répliquer le profil Secure Client (services client sécurisés) sur l'unité en veille, effectuez l'une des opérations suivantes :

  - Saisissez la commande **write standby** sur l'unité active.
  - Réappliquez le profil sur l'unité active.
  - Rechargez l'unité en veille.

- Autorités de certification (CA) locales
- Images ASA
- Images ASDM

Réplication de la commande

Après le démarrage, les commandes que vous saisissez sur l'unité active sont immédiatement répliquées sur l'unité de secours.Vous n'avez pas besoin d'enregistrer la configuration active dans la mémoire flash pour répliquer les commandes.

Dans le basculement actif/actif, les modifications saisies dans l'espace d'exécution du système sont répliquées à partir de l'unité sur laquelle le groupe de basculement 1 est à l'état actif.

Si lesmodifications ne sont pas saisies sur l'unité appropriée pour que la réplication des commandes puisse avoir lieu, les configurations ne seront plus synchronisées. Ces modifications pourraient être perdues lors de la prochaine synchronisation de la configuration initiale.

Les commandes suivantes sont répliquées sur l'ASA de secours :

- Toutes les commandes de configuration, à l'exception de **mode**, **firewall** et **failover lan unit**
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

Les commandes suivantes ne sont *pas* répliquées sur l'ASA de secours :

- Toutes les formes de la commande **copy**, à l'exception de **copy running-config startup-config**
- Toutes les formes de la commande **write**, à l'exception de **write memory**
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** et **pager**

Optimisation de la synchronisation de la configuration

L'optimisation de la synchronisation de configuration est une amélioration de la synchronisation de la configuration qui

- compare les valeurs de hachage de configuration entre les périphériques actifs et les périphériques en cours de connexion pour déterminer si une synchronisation complète est nécessaire
- permet au périphérique de rejoindre la grappe plus rapidement en ignorant la synchronisation complète de la configuration lorsque les valeurs de hachage correspondent, et
- réduit la fenêtre de maintenance et le temps de mise à niveau pendant les opérations de basculement à .

Lignes directrices et limitations de l'optimisation de la synchronisation de la configuration

Lorsqu'un périphérique redémarre ou rejoint la grappe après une suspension ou une reprise du basculement à , le périphérique qui rejoint la grappe efface sa configuration en cours d'exécution. Le périphérique actif envoie alors l'intégralité de sa configuration au périphérique en phase de jonction afin de synchroniser complètement les configurations. Si le périphérique actif a une configuration importante, ce processus peut prendre plusieurs minutes.

La fonctionnalité d'optimisation de la synchronisation de la configuration permet de comparer la configuration du périphérique en phase de jonction et du périphérique actif en échangeant des valeurs de hachage de configuration. Si le hachage calculé sur les périphériques actifs et en phase de jonction correspond, le périphérique en cours d'adhésion ignore la synchronisation complète de la configuration et rejoint la configuration du basculement. Cette fonctionnalité garantit un appairage plus rapide et réduit la fenêtre de maintenance ainsi que le temps de mise à niveau.

Lignes directrices et limitations :

- La fonctionnalité d'optimisation de la synchronisation de la configuration est activée par défaut.
- Le mode de contexte multiple de l'ASA prend en charge l'optimisation de la synchronisation de la configuration en partageant l'ordre des contextes lors de la synchronisation complète de la configuration, ce qui permet la comparaison de l'ordre des contextes lors de la jonction de nœuds suivante.
- Si vous configurez la phrase secrète et la clé IPsec de basculement, l'optimisation de la synchronisation de la configuration n'est pas effective, car la valeur de hachage calculée dans le périphérique actif et le périphérique en veille est différente.
- Si vous configurez le périphérique avec une ACL dynamique ou SNMPv3, l'optimisation de la synchronisation de la configuration n'est pas effective.
- Le périphérique actif synchronise la configuration complète avec le basculement des liaisons LAN comme comportement par défaut. Pendant les oscillations de basculement entre les périphériques actifs et en veille, l'optimisation de la synchronisation de la configuration n'est pas déclenchée et les périphériques effectuent une synchronisation complète de la configuration.
- L'optimisation de la synchronisation de la configuration est déclenchée lorsque la configuration du basculement récupère d'une interruption ou d'une perte de communication réseau entre les périphériques actifs et en veille.

Supervision de l'optimisation de la synchronisation de la configuration :

- Des messages syslog sont générés pour indiquer si les valeurs de hachage calculées sur l'unité active et en cours de jonction correspondent, ne correspondent pas ou si le délai de l'opération expire.
- Le message syslog affiche également le temps écoulé, depuis l'envoi de la demande de hachage jusqu'au moment d'obtenir et de comparer la réponse de hachage.

Commandes de supervision pour l'optimisation de la synchronisation de la configuration. Vous pouvez exécuter ces commandes en sélectionnant **Tools (Outils) » Command Line Interface (interface de ligne de commande)**.

- **show failover config-sync checksum** : affiche des informations sur l'état du périphérique et la somme de contrôle.
- **show failover config-sync configuration** : affiche des informations sur la configuration du périphérique et la somme de contrôle.

- **show failover config-sync status** : affiche l'état de la fonctionnalité d'optimisation de la synchronisation de la configuration.



Remarque La commande Configuration State in **show failover state** affiche l'état de synchronisation de la configuration pendant la jonction à haute accessibilité. Cet état ne reflète pas les déploiements ou modifications de configuration ultérieurs ni la réplication sur le périphérique tant qu'une resynchronisation n'a pas été lancée.

Basculement actif/de secours

Le basculement actif/veille est une configuration à haute accessibilité qui

- vous permet d'utiliser un périphérique ASA de secours pour reprendre les fonctionnalités d'une unité en panne,
- permet à l'unité en veille de devenir l'unité active lorsque l'unité active tombe en panne, et
- permet à l'unité défaillante de revenir en ligne en tant qu'unité de secours si le problème est temporaire.

L'unité défaillante doit être remplacée si le problème n'est pas temporaire. Définissez l'unité de secours comme unité principale avant de remplacer l'unité défectueuse pour conserver la configuration de l'unité secondaire.

Pour le mode de contexte multiple, l'ASA peut basculer l'unité entière (y compris tous les contextes), mais ne peut pas basculer des contextes individuels séparément.

Rôles principal/secondaire et état actif/de secours

Les rôles principaux/secondaires et l'état actif/en veille sont des concepts de configuration de basculement qui

- définissent la hiérarchie des unités, les unités principales prévalant lors du démarrage simultané
- déterminent les modèles d'utilisation des adresses IP et des adresses MAC pendant les opérations de basculement, et
- établissent les rôles de flux de trafic entre les unités jumelées dans les configurations de basculement actif/veille.

Différences entre les unités principale et secondaire

Les principales différences entre les deux unités d'une paire de basculement dépendent de l'unité active et de l'unité en veille, à savoir les adresses IP à utiliser et l'unité transmettant activement le trafic.

Cependant, il existe quelques différences entre les unités en fonction de l'unité principale (comme spécifié dans la configuration) et de l'unité secondaire :

- L'unité principale devient toujours l'unité active si les deux unités démarrent en même temps (et ont le même état de fonctionnement opérationnel).
- Les adresses MAC de l'unité principale sont toujours associées aux adresses IP actives. L'exception à cette règle se produit lorsque l'unité secondaire devient active et ne peut pas obtenir les adresses MAC

de l'unité principale sur la liaison de basculement. Dans ce cas, les adresses MAC des unités secondaires sont utilisées.

Détermination de l'unité active au démarrage

La détermination de l'unité active au démarrage est un processus de haute accessibilité qui

- définit une unité comme unité en veille si elle démarre et détecte un homologue qui fonctionne déjà comme unité active,
- définit une unité comme active si elle démarre et ne détecte pas d'homologue, et
- définit l'unité principale comme unité active et l'unité secondaire comme unité en veille si les deux unités démarrent simultanément.

Événements de basculement

Un événement de basculement est une condition du système qui

- déclenche une unité active pour transférer le contrôle à une unité de secours dans les configurations de basculement actif/veille
- se produit sur une base unitaire et ne peut pas basculer des contextes individuels ou des groupes de contextes même sur les systèmes exécutés en mode à contextes multiples, et
- suit des politiques de basculement spécifiques qui déterminent si un basculement se produit et quelles actions sont effectuées par chaque unité.

Politiques et actions d'événements de basculement

Le tableau suivant présente l'action de basculement pour chaque défaillance. Pour chaque défaillance, le tableau indique la politique de basculement (basculement ou absence de basculement), l'action prise par l'unité active, l'action entreprise par l'unité de secours, et toute remarque spéciale sur la condition et les actions de basculement.

Tableau 19 : Événements de basculement

Défaillance	Politique	Action de l'unité active	Action de l'unité de secours	Notes
Défaillance de l'unité active (alimentation ou matérielle)	Basculement	S.O.	Devenir active Marquer l'unité active comme défaillante	Aucun message Hello n'est reçu sur l'interface surveillée ou sur la liaison de basculement.
L'unité précédemment active récupère	Aucun basculement	Devient l'unité de secours	Aucune action	Aucun.
Défaillance de l'unité de secours (alimentation ou matériel)	Aucun basculement	Marquer l'unité de secours come défaillante	S.O.	Lorsque l'unité de secours est marquée comme défaillante, l'unité active ne tente pas de basculer, même si le seuil de défaillance de l'interface est dépassé.

Défaillance	Politique	Action de l'unité active	Action de l'unité de secours	Notes
Échec de la liaison de basculement pendant l'opération	Aucun basculement	Marquer la liaison de basculement comme défaillante	Marquer la liaison de basculement comme défaillante	Vous devez restaurer la liaison de basculement dès que possible, car l'unité ne peut pas basculer vers l'unité de secours lorsque la liaison de basculement est inactive.
Échec de la liaison de basculement au démarrage	Aucun basculement	Devenir active Marquer la liaison de basculement comme défaillante	Devenir active Marquer la liaison de basculement comme défaillante	Si la liaison de basculement est interrompue au démarrage, les deux unités deviennent actives.
Échec du lien avec l'état	Aucun basculement	Aucune action	Aucune action	Les informations d'état deviennent obsolètes et les sessions sont interrompues en cas de basculement.
Défaillance de l'interface sur l'unité active supérieure au seuil	Basculement	Marquer l'unité active comme défaillante	Devenir active	Aucun.
Défaillance de l'interface sur l'unité de secours supérieure au seuil	Aucun basculement	Aucune action	Marquer l'unité de secours come défaillante	Lorsque l'unité de secours est marquée comme en panne, l'unité active ne tente pas de basculer, même si le seuil de défaillance de l'interface est dépassé.

À propos du basculement actif/actif

Cette section décrit le basculement actif/actif.

Présentation du basculement actif/actif

Dans une configuration de basculement actif/actif, les deux ASA peuvent transmettre le trafic réseau. Le basculement actif/actif n'est disponible que pour les ASA en mode de contexte multiple. Dans le basculement actif/actif, vous divisez les contextes de sécurité sur l'ASA en un maximum de 2 groupes de basculement.

Un groupe de basculement est simplement un groupe logique d'un ou plusieurs contextes de sécurité. Vous pouvez attribuer un groupe de basculement actif sur l'ASA principal et un groupe de basculement 2 actif sur l'ASA secondaire. Lorsqu'un basculement se produit, il se produit au niveau du groupe de basculement. Par exemple, selon le modèle de défaillance d'interface, il est possible que le groupe de basculement 1 bascule vers l'ASA secondaire et que le groupe de basculement 2 bascule vers l'ASA principal. Cet événement peut se produire si les interfaces du groupe de basculement 1 sont inactives sur l'ASA principal, mais actives sur l'ASA secondaire, tandis que les interfaces du groupe de basculement 2 sont inactives sur l'ASA secondaire, mais actives sur l'ASA principal.

Le contexte d'administration est toujours membre du groupe de basculement 1. Tous les contextes de sécurité non attribués sont également membres du groupe de basculement 1 par défaut. Si vous souhaitez bénéficier d'un basculement actif/actif, mais que vous n'êtes pas intéressé par les contextes multiples, la configuration la plus simple serait d'ajouter un contexte supplémentaire et de l'affecter au groupe de basculement 2.

Remarque Lors de la configuration du basculement actif/actif, assurez-vous que le trafic combiné des deux unités entre dans la capacité de chacune d'elles.

Remarque Vous pouvez attribuer les deux groupes de basculement à un seul ASA si vous le souhaitez, mais vous ne profiterez pas de deux ASA actifs.

Rôles principal/secondaire et état actif/de secours pour un groupe de basculement

Comme pour le basculement actif/de secours, une unité d'une paire de basculement actif/actif est désignée comme l'unité principale et l'autre unité, comme l'unité secondaire. Contrairement au basculement actif/de secours, cette désignation n'indique pas quelle unité devient active lorsque les deux unités démarrent simultanément. Au lieu de cela, la désignation principale/secondaire fait deux choses :

- L'unité principale fournit la configuration d'exécution à la paire lorsqu'elles démarrent simultanément.
- Chaque groupe de basculement de la configuration est configuré avec une préférence d'unité principale ou secondaire. Lorsqu'elle est utilisée avec la préemption, cette préférence garantit que le groupe de basculement s'exécute sur la bonne unité après son démarrage. Sans préemption, les deux groupes s'exécutent sur la première unité de démarrage.

Détermination de l'unité active pour les groupes de basculement au démarrage

L'unité sur laquelle un groupe de basculement devient actif est déterminée comme suit :

- Lorsqu'une unité démarre alors que l'unité homologue n'est pas disponible, les deux groupes de basculement deviennent actifs sur l'unité.
- Lorsqu'une unité démarre alors que l'unité homologue est active (avec les deux groupes de basculement à l'état actif), les groupes de basculement restent à l'état actif sur l'unité active, quelle que soit la préférence principale ou secondaire du groupe de basculement jusqu'à ce que l'un des scénarios suivants se produise :
  - Un basculement se produit.
  - Un basculement est forcé manuellement.
  - Une préemption pour le groupe de basculement est configurée, ce qui fait que le groupe de basculement devient automatiquement actif sur l'unité préférée lorsque l'unité devient disponible.

Événements de basculement

Dans une configuration de basculement actif/actif, le basculement se produit sur la base d'un groupe de basculement, et non sur une base de système. Par exemple, si vous désignez les deux groupes de basculement comme actifs sur l'unité principale et que le groupe de basculement 1 échoue, le groupe de basculement 2 reste actif sur l'unité principale pendant que le groupe de basculement 1 devient actif sur l'unité secondaire.

Comme un groupe de basculement peut contenir plusieurs contextes et que chaque contexte peut contenir plusieurs interfaces, il est possible que toutes les interfaces d'un contexte unique tombent en panne sans entraîner la défaillance du groupe de basculement associé.

Le tableau suivant présente l'action de basculement pour chaque défaillance. Pour chaque événement de défaillance, la politique (que le basculement se produise ou non), les actions pour le groupe de basculement actif et les actions pour le groupe de basculement en veille sont données.

Tableau 20 : Événements de basculement

Défaillance	Politique	Action pour le groupe actif	Action pour le groupe en veille	Notes
Une unité subit une défaillance d'alimentation ou de logiciel	Basculement	Devient l'unité de secours Marquer comme défaillante	Devenir active Marquer l'unité active comme défaillante	Lorsqu'une unité d'une paire de basculement tombe en panne, tous les groupes de basculement actifs sur cette unité sont marqués comme défaillants et deviennent actifs sur l'unité homologue.
Défaillance de l'interface sur le groupe de basculement actif supérieure au seuil	Basculement	Marquer le groupe actif comme défaillant	Devenir active	Aucun.
Défaillance de l'interface sur le groupe de basculement en veille supérieure au seuil	Aucun basculement	Aucune action	Marquer le groupe en veille comme défaillant	Lorsque le groupe de basculement en veille est marqué comme défaillant, le groupe de basculement actif ne tente pas de basculer, même si le seuil de défaillance de l'interface est dépassé.
Le groupe de basculement anciennement actif récupère	Aucun basculement	Aucune action	Aucune action	À moins que la préemption de groupe de basculement ne soit configurée, les groupes de basculement restent actifs sur leur unité actuelle.
Échec de la liaison de basculement au démarrage	Aucun basculement	Devenir active	Devenir active	Si la liaison de basculement est interrompue au démarrage, les deux groupes de basculement sur les deux unités deviennent actifs.
Échec du lien avec l'état	Aucun basculement	Aucune action	Aucune action	Les informations d'état deviennent obsolètes et les sessions sont interrompues en cas de basculement.
Échec de la liaison de basculement pendant l'opération	Aucun basculement	S.O.	S.O.	Chaque unité marque la liaison de basculement comme défaillante. Vous devez restaurer la liaison de basculement dès que possible, car l'unité ne peut pas basculer vers l'unité de secours lorsque la liaison de basculement est inactive.

Licences pour le basculement

Pour la plupart des modèles, les unités de basculement ne nécessitent pas la même licence sur chaque unité. Si vous avez des licences sur les deux unités, elles se combinent en une seule licence de grappe de basculement d'exécution. Il y a certaines exceptions à cette règle. Consultez le tableau suivant pour connaître les exigences précises en matière de licence pour le basculement.

Modèle	Exigence de licence
ASA virtuel	Consultez Licences de basculement pour l'ASAv, à la page 137.
Firepower 1010	Licence Security Plus sur les deux unités. Consultez Licences de basculement pour Firepower 1010, à la page 137.
Firepower 1100	Consultez Licences de basculement pour Firepower 1100, à la page 138.
Firepower de la série 2100	Consultez Licences de basculement pour Firepower 2100, à la page 140.
Cisco Secure Firewall 3100	Consultez Licences de basculement pour Cisco Secure Firewall 3100, à la page 141.
Firepower 4100/9300	Consultez Licences de basculement pour le Firepower 4100/9300, à la page 143.
ISA 3000	Licence Security Plus sur les deux unités. **Remarque** Chaque unité doit avoir la même licence de chiffrement.

Remarque Une clé permanente valide est requise; dans de rares cas sur l'ISA 3000, votre clé d'authentification PAK peut être supprimée. Si votre clé est constituée uniquement de 0, vous devez réinstaller une clé d'authentification valide avant que le basculement puisse être activé.

Lignes directrices pour Basculement

Mode contextuel

- Le mode Actif/Actif est pris en charge uniquement en mode de contexte multiple.
- Pour le mode de contexte multiple, effectuez toutes les étapes dans l'espace d'exécution du système, sauf indication contraire.

Prise en charge des modèles

- / 1010/ :

- Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l'utilisation de Basculement. Étant donné que les ports de commutation fonctionnent dans le matériel, ils continuent de faire circuler le trafic sur les unités actives *et* en veille. Basculement est conçu pour empêcher le trafic de passer par l'unité en veille, mais cette fonctionnalité ne s'étend pas aux ports de commutation. Dans une configuration réseau Basculement normale, les ports de commutateur actifs sur les deux unités mèneront à des boucles réseau. Nous vous suggérons d'utiliser des commutateurs externes pour toute capacité de commutation. Notez que les interfaces VLAN peuvent être surveillées par basculement, contrairement aux ports de commutation. Théoriquement, vous pouvez mettre un port de commutation unique sur un réseau VLAN et utiliser Basculement avec succès, mais une configuration plus simple consiste à utiliser des interfaces physiques de pare-feu à la place.
- Vous ne pouvez utiliser qu'une interface de pare-feu comme liaison de basculement.

- Firepower 9300 : nous vous recommandons d'utiliser le basculement entre les châssis pour une redondance optimale.
- Les ASA virtuel sur les réseaux infonuagiques publics tels que Microsoft Azure et Amazon Web Services ne sont pas pris en charge par Basculement standard, car une connectivité de couche 2 est requise. Au lieu de cela, consultez Basculement pour la haute disponibilité dans le nuage public, à la page 345.

Basculement ASA virtuel pour la haute disponibilité

Lors de la création d'une paire de basculement à l'aide de l'ASA virtuel, il est nécessaire d'ajouter les interfaces de données à chaque ASA virtuel dans le même ordre. Si exactement les mêmes interfaces sont ajoutées à chaque ASA virtuel, mais dans un ordre différent, des erreurs peuvent s'afficher à la console ASA virtuel. La fonctionnalité de basculement peut également être affectée

Directives supplémentaires

- Lorsque l'unité active bascule sur l'unité en veille, le port du commutateur connecté exécutant le protocole Spanning Tree (STP) peut passer dans un état bloquant pendant 30 à 50 secondes lorsqu'il détecte le changement de topologie. Pour éviter la perte de trafic lorsque le port est dans un état bloquant, vous pouvez activer la fonctionnalité STP PortFast sur le commutateur :

  interface *interface_id* **spanning-tree portfast**

  Cette solution de contournement s'applique aux commutateurs connectés aux interfaces du mode routé et de groupe de ponts. La fonctionnalité PortFast fait immédiatement passer le port en mode de transfert STP lors de l'établissement de la liaison. Le port participe toujours à STP. Ainsi, si le port doit faire partie de la boucle, le port finit par passer en mode de blocage STP.
- La configuration de la sécurité des ports sur les commutateurs connectés à la paire de basculement ASA peut entraîner des problèmes de communication lors d'un basculement. Ce problème se produit lorsqu'une adresse MAC sécurisée configurée ou apprise sur un port sécurisé est déplacée vers un autre port sécurisé. Une violation est signalée par la fonctionnalité de sécurité du port du commutateur.
- Vous pouvez surveiller jusqu'à 1 025 interfaces sur une unité, dans tous les contextes.
- Pour un tunnel Basculement actif/en veille et un tunnel VPN IPsec, vous ne pouvez pas surveiller les unités active et en veille à l'aide de SNMP sur le tunnel VPN. L'unité de secours n'a pas de tunnel VPN actif et abandonnera le trafic destiné au système NMS. Vous pouvez plutôt utiliser SNMPv3 avec chiffrement pour que le tunnel IPsec ne soit pas requis.

- Lorsqu'aucun basculement n'est déclenché pendant un état actif/en veille intègre, aucune des interfaces de l'unité de secours n'est fermée. Toutefois, si cela se produit pendant que la haute accessibilité est dans un état actif/défaillance, toutes les interfaces, y compris l'interface de gestion, sont fermées sur l'unité défaillante, à l'exception du réseau local (LAN) de basculement et des interfaces d'état. Ainsi, il est nécessaire d'éviter d'éventuels problèmes de trafic si les interfaces défaillantes deviennent actives après la désactivation du basculement. Le réseau local (LAN) de basculement et les interfaces d'état restent opérationnels pour assurer une communication de basculement continue.
- Pour le basculement actif/actif, deux interfaces dans le même contexte ne doivent pas être configurées dans le même groupe ASR.
- Pour le basculement actif/actif, vous pouvez définir un maximum de deux groupes de basculement.
- Pour le basculement actif/actif, lors de la suppression de groupes de basculement, vous devez supprimer le groupe de basculement 1 en dernier. Le groupe de basculement1 contient toujours le contexte d'administration. Tout contexte non affecté à un groupe de basculement passe par défaut au groupe de basculement 1. Vous ne pouvez pas supprimer un groupe de basculement auquel des contextes sont affectés explicitement.
- Immédiatement après le basculement, l'adresse source des messages du journal système sera l'adresse de l'interface de basculement pendant quelques secondes.
- Pour une meilleure convergence (pendant un basculement), vous devez fermer les interfaces sur une paire à haute disponibilité qui ne sont associées à aucune configuration ou instance.
- Dans les déploiements à haute accessibilité avec des interfaces de basculement et d'état partagées, si la connectivité sur l'interface de basculement échoue alors que l'unité de secours est dans l'état de configuration synchronisée et que celle-ci passe ensuite à l'état actif, il en résulte un état de cerveau divisé. Cette situation est observée même lorsqu'il y a une interface surveillée.

  La connectivité sur l'interface de basculement peut échouer dans les situations suivantes :

  - Après le redémarrage de l'unité de secours, la connectivité sur l'interface de basculement tombe en panne, tandis que l'unité de secours est dans l'état de configuration de synchronisation.
  - Après avoir activé le basculement précédemment désactivé sur l'unité de secours, la connectivité sur l'interface de basculement échoue pendant que l'unité de secours est dans l'état de configuration synchronisé.

  Pour éviter l'état de cerveau divisé, utilisez les interfaces de basculement et d'état. Si les défaillances de connectivité sur les interfaces de basculement persistent, isolez la nouvelle unité active (anciennement de secours) du réseau.
- Si vous configurez le chiffrement de basculement en mode d'évaluation, les systèmes utilisent DES pour le chiffrement. Si vous enregistrez ensuite les périphériques à l'aide d'un compte compatible avec l'exportation, ils utiliseront AES après un redémarrage. Ainsi, si un système redémarre pour une raison quelconque, y compris après l'installation d'une mise à niveau, les homologues ne pourront pas communiquer et les deux unités deviendront l'unité active. Nous vous recommandons de ne pas configurer le chiffrement avant d'avoir enregistré les périphériques. Si vous configurez cela en mode d'évaluation, nous vous recommandons de supprimer le chiffrement avant d'enregistrer les périphériques.
- Lorsque vous utilisez SNMPv3 avec basculement, si vous remplacez une unité de basculement, les utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez rajouter les utilisateurs SNMPv3 à l'unité active pour forcer les utilisateurs à se reproduire sur la nouvelle unité; ou vous pouvez ajouter les utilisateurs directement sur la nouvelle unité. Reconfigurez chaque utilisateur en saisissant la

commande **snmp-server user** *username group-name* **v3** sur l'unité active ou directement sur l'unité de secours avec les options *priv-password* et *auth-password* dans leur format non chiffré.

- Le périphérique ne partage pas les données du moteur client SNMP avec son homologue.
- Si vous avez un très grand nombre de règles de contrôle d'accès et de NAT, la taille de la configuration peut empêcher une duplication efficace de la configuration, ce qui se traduit par le fait que l'unité de secours met trop de temps à atteindre l'état de veille. Cela peut également avoir une incidence sur votre capacité à vous connecter à l'unité de secours pendant la duplication via la console ou la session SSH. Pour améliorer les performances de duplication de la configuration, activez la validation transactionnelle pour les règles d'accès et la NAT à l'aide des commandes **asp rule-engine transactional-commit access-group** et **asp rule-engine transactional-commit nat**.
- Une unité d'une paire Basculement qui passe en rôle de secours synchronise son horloge avec celle de l'unité active.

  Exemple :

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby              Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config               Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- Les unités de Basculement ne synchronisent pas l'horloge de manière dynamique. Voici quelques exemples d'événements où la synchronisation a lieu :
  - Une nouvelle paire Basculement est créée.
  - La paire Basculement est défectueuse et recréée.
  - La communication sur la liaison de basculement a été interrompue et rétablie.
  - L'état de basculement a été modifié manuellement au niveau de l'interface de ligne de commande (CLI) .
- L'activation de Basculement force la suppression de toutes les routes et leur rajout après le passage de la progression de Basculement à l'état actif. Vous pourriez subir des pertes de connexion pendant cette phase.
- Si vous activez le basculement sur un périphérique autonome, les interfaces de données tombent en panne lors de la négociation du basculement, interrompant le trafic.
- Dans la configuration Basculement, les connexions de courte durée, généralement qui utilisent le port 53, sont fermées rapidement et ne sont jamais transférées ou synchronisées de la position active à la zone en veille, il peut donc y avoir une différence dans le nombre de connexions sur les deux périphériques Basculement. C'est un comportement attendu pour les connexions de courte durée. Vous pouvez essayer de comparer les connexions qui sont de longue durée (par exemple, plus de 30 à 60 secondes).
- Dans la configuration Basculement, les connexions amorces (demandes de connexion qui n'ont pas encore terminé le processus d'établissement de liaison à trois étapes) sont fermées rapidement et ne sont pas synchronisées entre les périphériques actifs et en veille. Cette conception garantit l'efficacité et la

sécurité du système à haute disponibilité. Pour cette raison, il pourrait y avoir une différence dans le nombre de connexions sur les deux périphériques Basculement, ce qui est attendu.

- Si la liaison LAN de basculement n'est pas connectée dos à dos, mais plutôt connectée par un ou plusieurs commutateurs, une défaillance dans le chemin intermédiaire peut faire que l'unité active perde la connectivité avec l'unité de secours, ce qui entraîne des états actif/veille incohérents. Bien que cela n'ait pas d'incidence sur la fonctionnalité Basculement, il est conseillé de vérifier et de récupérer le chemin de liaison de basculement entre les unités actives et de secours.

  Lorsque la liaison LAN de basculement est inactive, il n'est pas conseillé de déployer une configuration, car elle pourrait ne pas être répliquée sur l'unité homologue.
- Dans OSPF dans l'ASA, si un commutateur à proximité tombe en panne et si l'interface ASA est connectée au même commutateur, les interfaces du pare-feu tombent également en panne avec la défaillance du commutateur. Il s'agit d'un comportement attendu. Cela déclenchera un basculement de haute disponibilité, comme prévu.
- Dans OSPF, après un basculement, la connexion OSPF avec le périphérique homologue devient non valide. Mettez fin à la connexion non valide, puis établissez une nouvelle connexion OSPF.
- Si l'ASA en veille est connecté à un autre commutateur, par exemple, lorsque l'interface sera activée, les tables de routage seront différentes de celle de l'ASA actif. Cela entraînera une panne de courte durée (environ 15 à 17 secondes) jusqu'à ce que les routes et la contiguïté soient mises à jour.
- En mode transparent, si vous avez des problèmes avec l'unité active qui perd l'adresse MAC du routeur de secours (HSRP), créez un mappage statique pour l'adresse MAC.

Paramètres par défaut pour le basculement

Par défaut, la politique de basculement comprend les éléments suivants :

- Aucune réplication HTTP dans le basculement dynamique.
- La défaillance d'une seule interface entraîne le basculement.
- Le délai d'interrogation de l'interface est de 5 secondes.
- Le délai de rétention de l'interface est de 25 secondes.
- Le délai d'interrogation de l'unité est de 1 seconde.
- Le délai de rétention de l'unité est de 15 secondes.
- Les adresses MAC virtuelles sont désactivées en mode de contexte multiple.
- Supervision de toutes les interfaces physiques.

Configurer le basculement actif/de secours

Pour configurer le basculement actif/veille, configurez les paramètres de basculement de base sur les unités principale et secondaire. Toutes les autres configurations se produisent uniquement sur l'unité principale et sont ensuite synchronisées avec l'unité secondaire.

L'**assistant de haute disponibilité et d'évolutivité** vous guide dans un processus étape par étape de création d'une configuration de basculement actif/veille.

Procédure

Étape 1 Sélectionnez **Wizards (Assistants) > High Availability and Scalability Wizard (Assistant de haute disponibilité et d'évolutivité)**. Consultez les instructions relatives à l'assistant dans les étapes suivantes.

Étape 2 Dans l'écran **Failover Peer Connectivity and Compatibility** (Connectivité et compatibilité des homologues de basculement), saisissez l'adresse IP de l'unité homologue. Cette adresse doit être une interface sur laquelle l'accès ASDM est activé.

Par défaut, l'adresse homologue est définie comme adresse de veille pour l'interface de gestion ASDM.

Étape 3 Dans l'écran **LAN Link Configuration (Configuration du lien LAN)** :

- **Interface** : l'interface peut être une interface physique de données, une sous-interface, une ou un ID d'interface EtherChannel.Sur Firepower 1010, l'interface est un ID d'interface de pare-feu; vous ne pouvez pas spécifier d'ID de port de commutation ni d'ID de VLAN. Pour le Firepower 4100/9300, vous pouvez utiliser n'importe quelle interface de type de données.
- **Active IP Address (Adresse IP active)** : cette adresse doit se trouver sur un sous-réseau inutilisé. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.
- **Standby IP Address (Adresse IP en veille)** : cette adresse IP doit être sur le même réseau que l'adresse IP active.
- (Facultatif) **Communications Encryption (Chiffrement des communications)** : chiffrez les communications sur la liaison de basculement. **Remarque** : au lieu d'une clé secrète, nous vous recommandons d'utiliser une clé prépartagée IPsec, que vous pouvez configurer après avoir quitté l'assistant (voir Modifier la configuration du basculement, à la page 333).

Étape 4 Sur l'écran **State Link Configuration (Configuration de la liaison d'état)**, si vous choisissez une autre interface pour le basculement dynamique :

- **Active IP Address (Adresse IP active)** : cette adresse IP doit se trouver sur un sous-réseau inutilisé, différent de la liaison de basculement. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.
- **Standby IP Address (Adresse IP en veille)** : cette adresse IP doit être sur le même réseau que l'adresse IP active.

Étape 5 Après avoir cliqué sur **Finish (Terminer)**, l'assistant affiche l'écran **Waiting for Config Sync (En attente de la synchronisation de la configuration)**.

Une fois la période spécifiée terminée, l'assistant envoie la configuration de basculement à l'unité secondaire et vous voyez un écran d'information indiquant que la configuration de basculement est terminée.

- Si vous ne savez pas si le basculement est déjà activé sur l'unité secondaire, attendez la période spécifiée.
- Si vous savez que le basculement est déjà activé, cliquez sur **Skip configuring peer (Ignorer la configuration homologue)**.

- Si vous savez que l'unité secondaire n'est pas encore activée pour le basculement, cliquez sur **Stop waiting** *xx* **more seconds (Arrêter d'attendre xx secondes supplémentaires)**, et la configuration de démarrage du basculement est immédiatement envoyée à l'unité secondaire.

Configurer le basculement actif/actif

Cette section explique comment configurer le basculement actif/actif.

L'**assistant de haute disponibilité et d'évolutivité** vous guide dans un processus étape par étape de création d'une configuration de basculement actif/actif.

Procédure

Étape 1 Sélectionnez **Wizards (Assistants)** > **High Availability and Scalability Wizard (Assistant de haute disponibilité et d'évolutivité)**. Consultez les instructions relatives à l'assistant dans les étapes suivantes.

Étape 2 Dans l'écran **Failover Peer Connectivity and Compatibility Check (Vérification de la connectivité et de la compatibilité en cas de basculement homologue)**, l'adresse IP homologue doit être une interface sur laquelle l'accès ASDM est activé.

Par défaut, l'adresse homologue est définie comme adresse de veille de l'interface à laquelle ASDM est connecté.

Étape 3 Dans l'écran **Security Contexte Configuration (Configuration du contexte de sécurité)**, si vous êtes passé en mode de contexte multiple dans le cadre de l'assistant, vous ne verrez que le contexte d'administration. Vous pouvez ajouter d'autres contextes après avoir quitté l'assistant.

Étape 4 Dans l'écran **LAN Link Configuration (Configuration du lien LAN)** :

- **Interface** : l'interface peut être une interface physique de données, une sous-interface, une interface redondante ou un ID d'interface EtherChannel. Pour l'ASA 5506H-X uniquement, vous pouvez spécifier l'interface de gestion Management 1/1 comme liaison de basculement. Ce faisant, vous devez enregistrer la configuration, puis recharger le périphérique. Vous ne pouvez alors pas utiliser cette interface à la fois pour le basculement et pour le module ASA Firepower; le module requiert l'interface pour la gestion et vous ne pouvez l'utiliser que pour une seule fonction. Pour le Firepower 4100/9300, vous pouvez utiliser n'importe quelle interface de type de données.
- **Active IP Address (Adresse IP active)** : cette adresse doit se trouver sur un sous-réseau inutilisé. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.
- **Standby IP Address (Adresse IP en veille)** : cette adresse IP doit être sur le même réseau que l'adresse IP active.
- (Facultatif) **Communications Encryption (Chiffrement des communications)** : chiffrez les communications sur la liaison de basculement. **Remarque** : au lieu d'une clé secrète, nous vous recommandons d'utiliser une clé prépartagée IPsec, que vous pouvez configurer après avoir quitté l'assistant (voir Modifier la configuration du basculement, à la page 333).

Étape 5 Sur l'écran **State Link Configuration (Configuration de la liaison d'état)**, si vous choisissez une autre interface pour le basculement dynamique :

- **Active IP Address (Adresse IP active)** : cette adresse IP doit se trouver sur un sous-réseau inutilisé, différent de la liaison de basculement. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.
- **Standby IP Address (Adresse IP en veille)** : cette adresse IP doit être sur le même réseau que l'adresse IP active.

Étape 6 Après avoir cliqué sur **Finish (Terminer)**, l'assistant affiche l'écran **Waiting for Config Sync (En attente de la synchronisation de la configuration)**.

Une fois la période spécifiée terminée, l'assistant envoie la configuration de basculement à l'unité secondaire et vous voyez un écran d'information indiquant que la configuration de basculement est terminée.

- Si vous ne savez pas si le basculement est déjà activé sur l'unité secondaire, attendez la période spécifiée.
- Si vous savez que le basculement est déjà activé, cliquez sur **Skip configuring peer (Ignorer la configuration homologue)**.
- Si vous savez que l'unité secondaire n'est pas encore activée pour le basculement, cliquez sur **Stop** en attendant *xx* **secondes supplémentaires)**, et la configuration de démarrage du basculement est immédiatement envoyée à l'unité secondaire.

Configurer les paramètres de basculement facultatifs

Vous pouvez personnaliser les paramètres de basculement à votre guise.

Configurer les critères de basculement et les autres paramètres

Consultez Paramètres par défaut pour le basculement, à la page 323 pour connaître les paramètres par défaut pour de nombreux paramètres que vous pouvez modifier dans cette section. Pour le mode actif/actif, vous définissez la plupart des critères par groupe de basculement. Cette section comprend l'activation de la réplication HTTP par groupe de basculement pour le mode actif/actif; pour configurer la réplication HTTP pour le mode actif/veille, consultez Modifier la configuration du basculement, à la page 333.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte multiple.
- Pour la détection de transfert bidirectionnel (BFD) des fonctions de surveillance de l'intégrité des unités, consultez les limites suivantes :
  - Firepower 9300 et 4100 uniquement.
  - Actif/Veille uniquement.
  - Mode routé uniquement

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **Failover (Basculement)**.

Étape 2 Désactivez la possibilité d'apporter des modifications à la configuration directement sur l'unité ou le contexte en veille : sous l'onglet **Setup** (Configuration), cochez la case **Disable configuration changes on the standby unit** (Désactiver les modifications de configuration sur l'unité en veille).

Par défaut, les configurations sur l'unité/le contexte de veille sont autorisées avec un message d'avertissement.

Étape 3 Sous **BFD Health Check** (Vérification de l'intégrité de BFD), cliquez sur **Manage** (Gérer) pour définir un modèle de BFD à utiliser pour la détection de l'état de basculement. La surveillance régulière de l'unité peut déclencher de fausses alarmes lorsque l'utilisation du CPU est élevée. La méthode BFD est distribuée, de sorte qu'un CPU élevé n'affecte pas son fonctionnement.

La page **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BFD** > **Template (Modèle)** s'ouvre. Cliquez sur **Add** (Ajouter) pour créer un modèle de saut unique; le multisaut n'est pas pris en charge. Pour les paramètres d'intervalle, vous pouvez spécifier des millisecondes; les microsecondes ne sont pas prises en charge. Pour les détails du modèle, consultez Créer le modèle BFD, à la page 897.

Étape 4 Cliquez sur l'onglet **Criteria** (Critères).

Étape 5 Configurez les délais d'interrogation des unités :

Dans la zone **Failover Poll Times** (Délais d'interrogation du basculement) :

- **Unit Failover** (Unité de basculement) : le temps entre les messages Hello des unités. La plage est comprise entre 1 et 15 secondes ou entre 200 et 999 millisecondes.
- **Unit Hold Time** (Délai de rétention de l'unité) : définit le temps pendant lequel une unité doit recevoir un message Hello sur la liaison de basculement, sinon l'unité commence le processus de test de défaillance des homologues. La plage est comprise entre 1 et 45 secondes ou entre 800 et 999 millisecondes. Vous ne pouvez pas saisir une valeur inférieure à 3 fois le délai d'interrogation.

Remarque Les autres paramètres de ce volet s'appliquent uniquement au mode actif/veille. En mode actif/actif, vous devez configurer le reste des paramètres par groupe de basculement.

Étape 6 (Mode actif/actif uniquement) Cliquez sur l'onglet **Active/Active** (Actif/Actif), puis choisissez un groupe de basculement et cliquez sur **Edit** (Modifier).

Étape 7 (Mode actif/actif uniquement) Modifiez le rôle préféré du groupe de basculement lorsqu'il est utilisé avec la préemption : cliquez sur **Primary** (Principal) ou **Secondary** (Secondaire).

Si vous avez utilisé l'assistant, le groupe de basculement 1 est affecté à l'unité principale et le groupe de basculement 2 est affecté à l'unité secondaire. Si vous souhaitez une configuration non standard, vous pouvez spécifier différentes préférences d'unité si vous le souhaitez. Ces paramètres ne sont utilisés qu'en conjonction avec le paramètre de préemption. Les deux groupes de basculement deviennent actifs sur l'unité qui démarre en premier (même s'il semble qu'ils démarrent simultanément, une unité devient active en premier), malgré le paramètre principal ou secondaire du groupe.

Étape 8 (Mode actif/actif uniquement) Configurez la préemption du groupe de basculement : cochez la case **Preempt after booting with optional delay of** (Préempter après le démarrage avec délai facultatif de).

Les deux groupes de basculement deviennent actifs sur l'unité qui démarre en premier (même s'il semble qu'ils démarrent simultanément, une unité devient active en premier), malgré le paramètre principal ou secondaire du groupe.

Vous pouvez saisir une valeur de délai facultative, qui spécifie le nombre de secondes pendant lesquelles le groupe de basculement reste actif sur l'unité actuelle avant de devenir automatiquement actif sur l'unité désignée. Cette valeur peut être comprise entre 1 et 1 200.

Si vous basculez manuellement, l'option Preempt (Préempter) est ignorée.



Remarque Si le basculement dynamique est activé, la préemption est retardée jusqu'à ce que les connexions soient répliquées à partir de l'unité sur laquelle le groupe de basculement est actuellement actif.

Étape 9 Configurez l'**Interface Policy** (Politique d'interface) :

- **Number of failed interfaces that triggers failover** (Nombre d'interfaces défaillantes qui déclenchent le basculement) : définissez un nombre précis d'interfaces qui doivent être défaillantes pour déclencher le basculement, compris entre 1 et 250. Lorsque le nombre d'interfaces surveillées défaillantes dépasse la valeur que vous avez spécifiée, l'ASA bascule.
- **Percentage of failed interfaces that triggers failover** (Pourcentage d'interfaces défaillantes qui déclenchent le basculement) : définissez un pourcentage d'interfaces configurées qui doivent être défaillantes pour déclencher le basculement. Lorsque le nombre d'interfaces surveillées défaillantes dépasse le pourcentage que vous avez défini, l'ASA bascule.



Remarque N'utilisez pas l'option **Use system failover interface policy** (Utiliser la politique d'interface de basculement du système). Vous pouvez uniquement définir la politique par groupe pour le moment.

Étape 10 (Mode actif/veille) Configurez les délais d'interrogation des interfaces :

Dans la zone **Failover Poll Time** (Délai d'interrogation du basculement) :

- **Monitored Interfaces** (Interfaces surveillées) : spécifie le délai d'interrogation de l'interface : combien de temps attendre entre l'envoi de paquets Hello à l'homologue. La plage est comprise entre 1 et 15 secondes ou 500 et 999 millisecondes. La valeur par défaut est de 5 secondes.
- **Link State** (État de liaison) : par défaut, chaque ASA d'une paire de basculement vérifie l'état de liaison de ses interfaces toutes les 500 ms. Vous pouvez personnaliser le délai d'interrogation. Par exemple, si vous définissez le délai d'interrogation à 300 ms, l'ASA peut détecter une défaillance d'interface et déclencher le basculement plus rapidement. La plage est comprise entre 300 et 799 millisecondes.
- **Interface Hold Time** (Délai de rétention de l'interface) : définit le temps (sous forme de calcul) entre le dernier message Hello reçu de l'unité homologue et le début des tests d'interface pour déterminer l'intégrité de l'interface. Il définit également la durée de chaque test d'interface comme *délai d'attente*/16. Les valeurs valides sont comprises entre 5 et 75 secondes. La valeur par défaut est de 5 fois le délai d'interrogation. Vous ne pouvez pas saisir une valeur de délai de rétention inférieure à cinq fois le délai d'interrogation.

Pour calculer le temps avant le début des tests d'interface (y) :

1. x = (*durée d'attente*/*durée d'interrogation*)/2, arrondi à l'entier le plus proche. (0,4 et moins sont arrondis à l'unité inférieure; 0,5 et plus sont arrondis à l'unité supérieure).
2. y = x**durée d'interrogation*

Par exemple, si vous utilisez le délai d'attente par défaut de 25 et le délai d'interrogation de 5, alors y = 15 secondes.

Pour le mode actif/actif, configurez les délais d'interrogation des interfaces dans la boîte de dialogue **Add/Edit Failover Group** (Ajouter/modifier le groupe de basculement).

Étape 11 (Mode actif/actif uniquement) Activez la réplication HTTP : cochez la case **Enable HTTP replication** (Activer la réplication HTTP).

Consultez la section Modifier la configuration du basculement, à la page 333 pour connaître le taux de réplication de la session.

Remarque En raison d'un retard lors de la suppression des flux HTTP de l'unité de secours lors de l'utilisation du basculement, la sortie **show conn count** pourrait afficher des numéros différents sur l'unité active par rapport à l'unité de secours; si vous attendez plusieurs secondes et réexécutez la commande, vous verrez le même nombre sur les deux unités.

Étape 12 Configurez des adresses MAC virtuelles :

- Mode active/veille : cliquez sur l'onglet **MAC Addresses** (Adresses MAC), puis sur **Add** (Ajouter).

  La boîte de dialogue **Add/Edit Interface MAC Address** (Ajouter/modifier une adresse MAC pour l'interface) s'affiche.

- Mode actif/actif : accédez au bas de l'onglet **Active/Active** (Actif/Actif).

Vous pouvez également définir l'adresse MAC à l'aide d'autres méthodes, mais nous vous conseillons d'utiliser une seule méthode. Si vous définissez l'adresse MAC à l'aide de plusieurs méthodes, l'adresse MAC utilisée dépend de nombreuses variables et peut ne pas être prédictible.

a) Choisissez une interface dans la liste déroulante **Physical Interface** (Interface physique).
b) Dans le champ **Active MAC Address** (Adresse MAC active), saisissez la nouvelle adresse MAC pour l'interface active.
c) Dans le champ **Standby MAC Address** (Adresse MAC en veille), saisissez la nouvelle adresse MAC pour l'interface en veille.
d) Cliquez sur **OK**. (Mode actif/actif uniquement) Cliquez à nouveau sur **OK**.

Étape 13 Cliquez sur **Apply** (Appliquer).

Configurer la supervision de l'interface et les adresses en veille

Par défaut, la supervision est activée sur toutes les interfaces physiques, ou pour le Firepower 1010, toutes les interfaces VLAN.Les ports de commutation Firepower 1010 ne sont pas admissibles à la surveillance d'interface.

Vous pourriez souhaiter empêcher les interfaces connectées à des réseaux moins critiques d'affecter votre politique de basculement.

Vous pouvez superviser jusqu'à 1 025 interfaces sur une unité (dans tous les contextes en mode de contexte multiple).

Si vous n'avez pas configuré les adresses IP de veille dans l'assistant, vous pouvez les configurer manuellement.

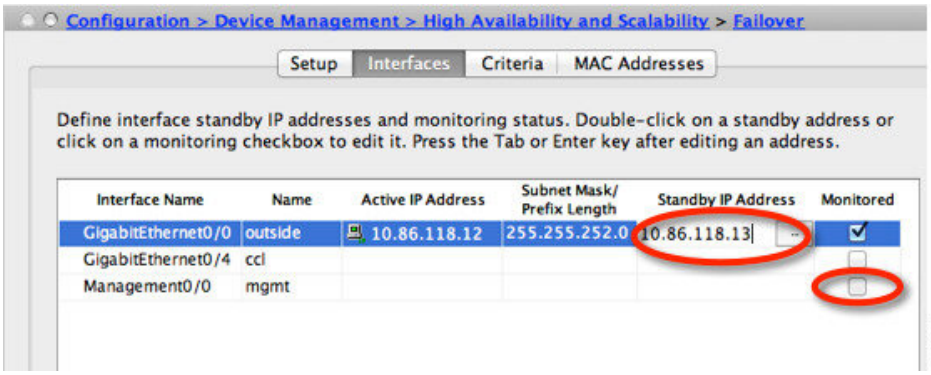
Avant de commencer

En mode de contexte multiple, configurez les interfaces dans chaque contexte.

Procédure

Étape 1 En mode unique, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability (Haute disponibilité)** > **Failover (Basculement)** > **Interfaces**.

En mode de contexte multiple, dans un contexte choisissez **Configuration > Device Management (Gestion des périphériques) > Failover (Basculement) > Interfaces**



Une liste des interfaces configurées s'affiche. La colonne **Monitored** (Sous surveillance) indique si une interface est surveillée ou non dans le cadre de vos critères de basculement. Si elle est surveillée, une coche apparaît dans la case **Monitored** (Sous surveillance).

L'adresse IP de chaque interface apparaît dans la colonne **Active IP Address** (Adresse IP active). Si elle est configurée, l'adresse IP en veille de l'interface apparaît dans la colonne **Standby IP Address** (Adresse IP en veille). La liaison de basculement et la liaison d'état n'affichent pas d'adresse IP; vous ne pouvez pas modifier ces adresses à partir de cet onglet.

Étape 2 Pour désactiver la surveillance d'une interface répertoriée, décochez la case **Monitored** (Sous surveillance) de l'interface.

Étape 3 Pour activer la surveillance d'une interface répertoriée, cochez la case **Monitored** (Sous surveillance) de l'interface.

Étape 4 Pour chaque interface qui n'a pas d'adresse IP en veille, cliquez deux fois sur le champ **Standby IP Address** (Adresse IP en veille) et saisissez une adresse IP dans le champ.

Si vous utilisez un filtre d'adresse locale de 31 bits pour les connexions point à point, ne configurez pas d'adresse IP en veille.

Étape 5 Cliquez sur **Apply** (Appliquer).

Configurer la prise en charge des paquets routés asymétriques (mode actif/actif)

Lorsqu'elle fonctionne en mode de basculement actif/actif, une unité peut recevoir un paquet de retour pour une connexion provenant de son unité homologue. Comme l'ASA qui reçoit le paquet n'a aucune information de connexion pour le paquet, le paquet est abandonné. Cet abandon se produit le plus généralement lorsque les deux ASA d'une paire de basculement actif/actif sont connectés à des fournisseurs de services différents et que la connexion sortante n'utilise pas d'adresse NAT.

Vous pouvez empêcher l'abandon des paquets de retour en autorisant les paquets routés de manière asymétrique. Pour ce faire, vous attribuez les interfaces similaires sur chaque ASA au même groupe ASR. Par exemple, les deux ASA se connectent au réseau interne sur l'interface interne, mais se connectent à des fournisseurs de services Internet distincts sur l'interface externe. Sur l'unité principale, affectez le contexte actif externe à l'interface au groupe ASR 1; sur l'unité secondaire, affectez le contexte actif en dehors de l'interface au même groupe ASR 1. Lorsque l'unité principale externe reçoit un paquet pour lequel elle n'a aucune information de session, elle vérifie les renseignements de session pour les autres interfaces dans les contextes de veille qui sont dans le même groupe; dans ce cas, le groupe ASR 1. Si elle ne trouve aucune correspondance, le paquet est abandonné. Si elle trouve une correspondance, l'une des actions suivantes se produit :

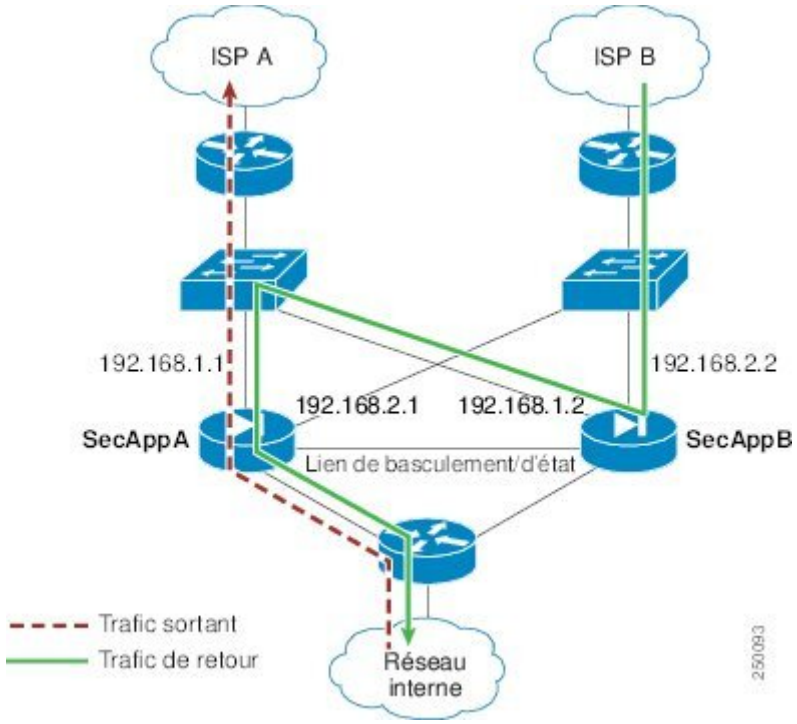
- Si le trafic entrant provient d'une unité homologue, tout ou partie de l'en-tête de couche 2 est réécrit et le paquet est redirigé vers l'autre unité. Cette redirection se poursuit tant que la session est active.
- Si le trafic entrant provient d'une interface différente sur la même unité, une partie ou la totalité de l'en-tête de couche 2 est réécrit et le paquet est réinjecté dans le flux.



Remarque Cette fonctionnalité ne fournit pas de routage asymétrique; elle restaure les paquets routés de manière asymétrique vers la bonne interface.

La figure suivante montre un exemple de paquet routé de manière asymétrique.

Illustration 54 : Exemple ASR



1. Une session sortante passe par l'ASA avec le contexte SecAppA actif. Elle quitte l'interface en dehors du FAI-A (192.168.1.1).
2. En raison d'un routage asymétrique configuré quelque part en amont, le trafic de retour passe par l'interface externe du FAI-B (192.168.2.2) sur l'ASA avec le contexte SecAppB actif.
3. Normalement, le trafic de retour serait abandonné, car il n'y a aucune information de session pour le trafic sur l'interface 192.168.2.2. Cependant, l'interface est configurée dans le cadre du groupe ASR 1. L'unité recherche la session sur toute autre interface configurée avec le même ID de groupe ASR.
4. Les renseignements de session se trouvent sur l'interface externe du FAI-A (192.168.1.2), qui est en état de veille sur l'unité avec SecAppB. Le basculement dynamique a répliqué les renseignements de session de SecAppA à SecAppB.
5. Au lieu d'être abandonné, l'en-tête de couche 2 est réécrit avec les renseignements pour l'interface 192.168.1.1 et le trafic est redirigé hors de l'interface 192.168.1.2, où il peut ensuite revenir par l'interface de l'unité à partir de laquelle il provient (192.168.1.1. sur SecAppA). Ce transfert se poursuit au besoin jusqu'à la fin de la session.

Avant de commencer

- Basculement dynamique : transmet les renseignements relatifs à l'état de session sur les interfaces du groupe de basculement actif au groupe de basculement de secours.
- HTTP de réplication : les renseignements relatifs à l'état de session HTTP ne sont pas transmis au groupe de basculement de secours et ne sont donc pas présents sur l'interface de secours. Pour que l'ASA puisse réacheminer les paquets HTTP routés de manière asymétrique, vous devez répliquer les renseignements relatifs à l'état HTTP.

- Effectuez cette procédure dans chaque contexte actif sur les unités principale et secondaire.
- Vous ne pouvez pas configurer à la fois des groupes ASR et des zones de trafic dans un contexte. Si vous configurez une zone dans un contexte, aucune des interfaces de contexte ne peut faire partie d'un groupe ASR.

Procédure

Étape 1 Dans le contexte actif de l'unité principale, choisissez **Configuration** > **Device Setup (Configuration des périphériques)** > **Routing (Routage)** > **ASR Groups (Groupes ASR)**.

Étape 2 Pour l'interface qui reçoit des paquets routés de manière asymétrique, choisissez un **ASR Group ID** (ID de groupe ASR) dans la liste déroulante.

Étape 3 Cliquez sur **Apply** (Appliquer) pour enregistrer vos modifications dans la configuration en cours d'exécution.

Étape 4 Connectez ASDM à l'unité secondaire et choisissez le contexte actif similaire au contexte de l'unité principale.

Étape 5 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **ASR Groups (Groupes ASR)**.

Étape 6 Pour l'interface similaire sur cette unité, choisissez le même **ASR Group ID** (ID de groupe ASR).

Étape 7 Cliquez sur **Apply** (Appliquer) pour enregistrer vos modifications dans la configuration en cours d'exécution.

Gérer Basculement

Cette section décrit comment gérer les unités Basculement après avoir activé Basculement, y compris comment modifier la configuration Basculement et comment forcer le basculement d'une unité à une autre.

Modifier la configuration du basculement

Si vous n'utilisez pas l'assistant ou si vous souhaitez modifier un paramètre, vous pouvez configurer la configuration de basculement manuellement. Cette section comprend également les options suivantes, qui ne sont pas incluses dans l'assistant; vous devez donc les configurer manuellement :

- Clé prépartagée IPsec pour le chiffrement du trafic de basculement
- Taux de réplication HTTP
- Réplication HTTP (mode actif/veille)

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 En mode unique, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **Failover (Basculement)** > **Setup (Configuration)**.

En mode de contexte multiple, choisissez **Configuration > Device Management (Gestion des périphériques) > Failover (Basculement) > Setup (Configuration)** dans l'espace d'exécution du système.

Étape 2 Cochez la case **Enable Failover** (Activer le basculement).

Remarque Le basculement n'est pas activé jusqu'à ce que vous appliquiez vos modifications au périphérique.

Étape 3 Pour chiffrer les communications sur les liaisons de basculement et d'état, utilisez l'une des options suivantes :

- **IPsec Preshared Key** (Clé prépartagée IPsec) (privilégié) : la clé prépartagée est utilisée par IKEv2 pour établir des tunnels IPsec LAN à LAN sur les liaisons de basculement entre les unités de basculement. Remarque : les tunnels de basculement LAN à LAN ne sont pas pris en compte dans la licence IPsec (autre VPN).
- **Secret Key** (Clé secrète) : saisissez la clé secrète utilisée pour chiffrer la communication de basculement. Si vous laissez ce champ vide, la communication de basculement, y compris tous les mots de passe ou clés de la configuration qui sont envoyés lors de la réplication des commandes, sera en texte clair.

  Use 32 hexadecimal character key (Utiliser la clé de 32 caractères hexadécimaux) : pour utiliser une clé de 32 caractères hexadécimaux pour la clé secrète, cochez cette case.

Étape 4 Dans la zone **LAN Failover** (Basculement LAN), définissez les paramètres suivants pour la liaison de basculement :

- **Interface** : choisissez l'interface à utiliser pour la liaison de basculement. Le basculement nécessite une interface dédiée, mais vous pouvez partager l'interface avec le basculement dynamique.

  Seules les interfaces ou sous-interfaces non configurées s'affichent dans cette liste et peuvent être sélectionnées comme liaison de basculement. Une fois que vous avez précisé une interface comme liaison de basculement, vous ne pouvez pas modifier cette interface dans le volet Configuration > Interfaces.
- **Logical Name** (Nom logique) : spécifiez le nom logique de l'interface utilisée pour la communication de basculement, par exemple « basculement ». Ce nom est fourni à titre informatif.
- **Active IP** (Adresse IP active) : spécifiez l'adresse IP active pour l'interface. L'adresse IP peut être une adresse IPv4 ou IPv6. Cette adresse IP doit se trouver sur un sous-réseau inutilisé.
- **Standby IP** (Adresse IP en veille) : spécifiez l'adresse IP en veille de l'interface, sur le même sous-réseau que l'adresse IP active.
- **Subnet Mask** (Filtre d'adresse locale) : spécifiez le filtre d'adresse locale.
- **Preferred Role** (Rôle privilégié) : sélectionnez **Primary** (Principal) ou **Secondary** (Secondaire) pour préciser si le rôle privilégié pour cet ASA est l'unité principale ou secondaire.

Étape 5 (Facultatif) Configurez la liaison d'état en procédant comme suit :

- **Interface** : choisissez l'interface à utiliser pour la liaison d'état. Vous pouvez choisir une interface ou une sous-interface non configurée, la liaison de basculement ou l'option **--Use Named--**.



Remarque Nous vous conseillons d'utiliser deux interfaces dédiées distinctes pour la liaison de basculement et la liaison d'état.

Si vous choisissez une interface ou une sous-interface non configurée, vous devez remplir les champs **Active IP** (Adresse IP active), **Subnet Mask** (Filtre d'adresse locale), **Logical Name** (Nom logique) et **Standby IP** (Adresse IP en veille) pour l'interface.

Si vous choisissez la liaison de basculement, vous n'avez pas besoin de préciser les valeurs **Active IP** (Adresse IP active), **Subnet Mask** (Filtre d'adresse locale), **Logical Name** (Nom logique) et **Standby IP** (Adresse IP en veille); les valeurs spécifiées pour la liaison de basculement sont utilisées.

Si vous choisissez l'option **--Use Named--**, le champ Logical Name (Nom logique) devient une liste déroulante d'interfaces nommées. Choisissez l'interface dans cette liste. Les valeurs **Active IP** (Adresse IP active), **Subnet Mask/Prefix Length (Longueur du filtre d'adresse locale/préfixe)** et **Standby IP** (Adresse IP en veille) n'ont pas besoin d'être spécifiées. Les valeurs spécifiées pour l'interface sont utilisées.

- **Logical Name** (Nom logique) : spécifiez le nom logique de l'interface utilisée pour la communication d'état, par exemple « état ». Ce nom est fourni à titre informatif.
- **Active IP** (Adresse IP active) : spécifiez l'adresse IP active pour l'interface. L'adresse IP peut être une adresse IPv4 ou IPv6. Cette adresse IP doit se trouver sur un sous-réseau inutilisé, différent de la liaison de basculement.
- **Standby IP** (Adresse IP en veille) : spécifiez l'adresse IP en veille de l'interface, sur le même sous-réseau que l'adresse IP active.
- **Subnet Mask** (Filtre d'adresse locale) : spécifiez le filtre d'adresse locale.
- (Facultatif, actif/veille uniquement) **Enable HTTP Replication** (Activer la réplication HTTP) : cette option permet au basculement dynamique de copier les sessions HTTP actives sur le pare-feu de secours. Si vous n'autorisez pas la réplication HTTP, les connexions HTTP sont déconnectées en cas de basculement. En mode actif/actif, définissez la réplication HTTP par groupe de basculement.



Remarque En raison d'un retard lors de la suppression des flux HTTP de l'unité de secours lors de l'utilisation du basculement, la sortie **show conn count** pourrait afficher des numéros différents sur l'unité active par rapport à l'unité de secours; si vous attendez plusieurs secondes et réexécutez la commande, vous verrez le même nombre sur les deux unités.

Étape 6 Dans la zone **Replication** (Réplication), définissez le taux de réplication de session en connexions par seconde. Les taux minimum et maximum sont déterminés par votre modèle. La valeur par défaut est le taux maximum. Pour utiliser la valeur par défaut, cochez la case **Use Default** (Utiliser la valeur par défaut).

Étape 7 Cliquez sur **Apply** (Appliquer).

La configuration est enregistrée sur le périphérique.

Étape 8 Si vous activez le basculement, une boîte de dialogue s'affiche pour configurer l'homologue de basculement.

- Cliquez sur **No** (Non) si vous souhaitez vous connecter ultérieurement à l'homologue de basculement et configurer les paramètres correspondants manuellement.
- Cliquez sur **Yes** (Oui) pour permettre à ASDM de configurer automatiquement les paramètres de basculement pertinents sur l'homologue de basculement. Saisissez l'adresse IP homologue dans le champ **Peer IP Address** (Adresse IP homologue).

Forcer le basculement

Pour forcer l'unité en veille à devenir active, procédez comme suit.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Pour forcer le basculement au niveau de l'unité :

a) Choisissez l'écran selon votre mode de contexte :

- En mode de contexte unique, choisissez **Monitoring (Supervision) > Properties (Propriétés) > Failover (Basculement) > Status (État)**.
- En mode de contexte multiple, dans le système, choisissez **Monitoring (Supervision) > Failover (Basculement) > System (Système)**.

b) Cliquez sur l'un des boutons suivants :

- Cliquez sur **Make Active** (Rendre actif) pour activer cette unité.
- Cliquez sur **Make Standby** (Mettre en veille) pour rendre l'autre unité active.

Étape 2 (Mode actif/actif uniquement) Pour forcer le basculement au niveau du groupe de basculement :

a) Dans le système, choisissez **Monitoring (Supervision) > Failover (Basculement) > Failover Group (Groupe de basculement)#**, où # correspond au numéro du groupe de basculement que vous souhaitez contrôler.

b) Cliquez sur l'un des boutons suivants

- Cliquez sur **Make Active** (Rendre actif) pour activer le groupe de basculement sur cette unité.
- Cliquez sur **Make Standby** (Mettre en veille) pour activer le groupe de basculement sur l'autre unité.

Désactiver le basculement

La désactivation du basculement sur une ou les deux unités permet de maintenir l'état actif et de veille de chaque unité jusqu'à ce que vous rechargiez. Pour une paire de basculement actif/actif, les groupes de basculement restent à l'état actif sur l'unité où ils sont actifs, quelle que soit l'unité pour laquelle ils sont configurés en priorité.

Affichez les caractéristiques suivantes lorsque vous désactivez le basculement :

- L'unité ou le contexte en veille reste en mode veille pour que les deux unités ne commencent pas à transmettre du trafic (cela s'appelle un état de pseudo-veille).
- L'unité ou le contexte en veille continue d'utiliser ses adresses IP en veille même s'il n'est plus connecté à une unité ou un contexte actif.
- L'unité ou le contexte en veille continue d'écouter une connexion sur la liaison de basculement. Si le basculement est réactivé sur l'unité ou le contexte actif, l'unité ou le contexte en veille reprend son état de veille ordinaire après avoir resynchronisé le reste de sa configuration.
- N'activez pas le basculement manuellement sur l'unité en veille; consultez plutôt Forcer le basculement, à la page 336. Si vous activez le basculement sur l'unité en veille, vous verrez un conflit d'adresses MAC qui peut perturber le trafic IPv6.
- Pour vraiment désactiver le basculement, enregistrez la configuration sans basculement dans la configuration de démarrage, puis rechargez.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 En mode unique, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **Failover (Basculement)** > **Setup (Configuration)**.

En mode de contexte multiple, choisissez **Configuration > Device Management (Gestion des périphériques) > Failover (Basculement) > Setup (Configuration)** dans l'espace d'exécution du système.

Étape 2 Décochez la case **Enable Failover** (Activer le basculement).

Étape 3 Cliquez sur **Apply** (Appliquer).

Étape 4 Pour désactiver complètement le basculement, enregistrez la configuration et rechargez :

a) Cliquez sur le bouton **Save** (enregistrer).

b) Choisissez **Tools (Outils) > System Reload (Rechargement du système)** pour recharger l'ASA.

Restaurer une unité défaillante

Pour restaurer une unité défaillante à un état sans échec, effectuez la procédure suivante.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Pour restaurer le basculement au niveau de l'unité :

a) Choisissez l'écran selon votre mode de contexte :

- En mode de contexte unique, choisissez **Monitoring (Supervision) > Properties (Propriétés) > Failover (Basculement) > Status (État)**.
- En mode de contexte multiple, dans le système, choisissez **Monitoring (Supervision) > Failover (Basculement) > System (Système)**.

b) Cliquez sur **Reset Basculement** (Réinitialiser le basculement).

Étape 2 (Mode actif/actif uniquement) Pour réinitialiser le basculement au niveau du groupe de basculement :

a) Dans le système, choisissez **Monitoring (Supervision) > Failover (Basculement) > Failover Group (Groupe de basculement)#**, où # correspond au numéro du groupe de basculement que vous souhaitez contrôler.

b) Cliquez sur **Reset Basculement** (Réinitialiser le basculement).

Resynchroniser la configuration

Les commandes répliquées sont stockées dans la configuration en cours d'exécution. Pour enregistrer les commandes répliquées dans la mémoire flash de l'unité en veille, sélectionnez **File (Fichier) > Save Running Configuration to Flash (Enregistrer la configuration en cours d'exécution dans la mémoire flash)**.

Remarque Si la limite maximale d'interface est atteinte, le nombre de tunnels VPN sur les unités active et en veille peut être incohérent. Dans cette situation, exécutez la commande **write standby** sur l'unité active pour synchroniser la configuration.

Surveillance de Basculement

La supervision Basculement est une fonctionnalité du système qui vous permet d'afficher l'état Basculement.

Messages de basculement

Lorsqu'un basculement se produit, les deux ASA envoient des messages système.

Messages de journal système de basculement

L'ASA émet un certain nombre de messages de journal système liés au basculement au niveau de priorité 2, ce qui indique une condition critique. Pour afficher ces messages, consultez le guide des messages du journal système. Les plages d'identifiants de message associés au basculement sont les suivantes : 101xxx, 102xxx, 103xxx, 104xxx, 105xxx, 210xxx, 311xxx, 709xxx et 727xxx. Par exemple, 105032 et 105043 indiquent un problème avec la liaison de basculement.



Remarque Pendant le basculement, l'ASA s'éteint de manière logique, puis affiche des interfaces, générant les messages de journal système 411001 et 411002. Il s'agit d'une activité normale.

Messages de débogage de basculement

Pour afficher les messages de débogage, saisissez la commande **debug fover**. Consultez la référence de commande pour en savoir plus.



Remarque Étant donné que la sortie de débogage se voit attribuer une priorité élevée dans le processus du CPU, elle peut affecter considérablement les performances du système. Par conséquent, les commandes **debug fover** doivent uniquement être utilisées pour résoudre des problèmes spécifiques ou au cours de sessions de dépannage effectuées avec le TAC de Cisco.

Interruptions de basculement SNMP

Pour recevoir des alertes SNMP de journal système pour le basculement, configurez l'agent SNMP pour envoyer des alertes SNMP aux stations de gestion SNMP, définissez un hôte de journal système et compilez la MIB de journal système Cisco dans votre station de gestion SNMP.

Supervision de l'état du basculement



Remarque Après un événement de basculement, vous devez soit lancer à nouveau ASDM, soit passer à un autre périphérique dans le volet Devices (Périphériques), puis revenir à l'ASA d'origine pour continuer à superviser le périphérique. Cette action est nécessaire, car la connexion de surveillance n'est pas rétablie lorsque ASDM est déconnecté, puis reconnecté au périphérique.

Choisissez **Monitoring (Supervision) > Properties (Propriétés) > Failover (Basculement)** pour superviser le basculement actif/veille.

Utilisez les écrans suivants dans la zone **Monitoring (Supervision) > Properties (Propriétés) > Failover (Basculement)** pour superviser le basculement actif/actif.

Système

Le volet System (Système) affiche l'état de basculement du système. Vous pouvez également contrôler l'état de basculement du système en :

- Basculant entre l'état actif et l'état de veille du périphérique.
- Réinitialisant un périphérique défaillant.
- Rechargeant l'unité de veille.

Champs

État de basculement du système : *affichage uniquement*. Affiche l'état de basculement de l'ASA. Les renseignements affichés sont les mêmes que ceux que vous pourriez recevoir de la commande **show failover**. Reportez-vous à la référence de commande pour en savoir plus sur la sortie affichée.

Les actions suivantes sont disponibles dans le volet System (Système) :

- Make Active (Rendre actif) : cliquez sur ce bouton pour faire de l'ASA l'unité active dans une configuration active/veille. Dans une configuration active/active, cliquez sur ce bouton pour que les deux groupes de basculement deviennent actifs sur l'ASA.
- Make Standby (Mettre en veille) : cliquez sur ce bouton pour faire de l'ASA l'unité de veille d'une paire active/veille. Dans une configuration active/active, cliquez sur ce bouton pour faire passer les deux groupes de basculement en état de veille sur l'ASA.
- Reset Failover (Réinitialiser le basculement) : cliquez sur ce bouton pour réinitialiser un système de l'état de défaillance à l'état de veille. Vous ne pouvez pas réinitialiser un système à l'état actif. Cliquer sur ce bouton sur l'unité active réinitialise l'unité de veille.
- Reload Standby (Recharger l'unité de veille) : cliquez sur ce bouton pour forcer l'unité de veille à se recharger.
- Refresh (Actualiser) : cliquez sur ce bouton pour actualiser les informations d'état dans le champ Failover state (État de basculement) du système.

Groupe de basculement 1 et groupe de basculement 2

Les volets Failover Group 1 (Groupe de basculement 1) et Failover Group 2 (Groupe de basculement 2) affichent l'état de basculement du groupe sélectionné. Vous pouvez également contrôler l'état de basculement du groupe en faisant basculer l'état actif/veille du groupe ou en réinitialisant un groupe défaillant.

Champs

État de basculement du groupe[*x*] :*affichage uniquement*. Affiche l'état de basculement du groupe de basculement sélectionné. Les renseignements affichés sont les mêmes que ceux que vous pourriez recevoir de la commande **show failover group** .

Vous pouvez effectuer les actions suivantes à partir de ce volet :

- Make Active (Rendre actif) : cliquez sur ce bouton pour activer le groupe de basculement sur l'ASA.
- Make Standby (Mettre en veille) : cliquez sur ce bouton pour forcer le groupe de basculement à entrer en état de veille sur l'ASA.
- Reset Failover (Réinitialiser le basculement) : cliquez sur ce bouton pour réinitialiser un système de l'état de défaillance à l'état de veille. Vous ne pouvez pas réinitialiser un système à l'état actif. Cliquer sur ce bouton sur l'unité active réinitialise l'unité de veille.

- Refresh (Actualiser) : cliquez sur ce bouton pour actualiser les informations d'état dans le champ Failover state (État de basculement) du système.

Historique de basculement

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Basculement actif/de secours	7.0(1)	Cette fonctionnalité a été introduite.
Basculement actif/actif	7.0(1)	Cette fonctionnalité a été introduite.
Prise en charge d'une valeur hexadécimale pour la clé de basculement	7.0(4)	Vous pouvez maintenant spécifier une valeur hexadécimale pour le chiffrement de la liaison de basculement. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > High Availability (Haute disponibilité) > Failover (Basculement) > Setup (Configuration).
Prise en charge de la phrase secrète principale pour la clé de basculement	8.3(1)	La clé de basculement prend désormais en charge la phrase secrète principale, qui chiffre la clé partagée dans la configuration de démarrage. Si vous copiez le secret partagé d'un ASA à un autre, par exemple à partir de la commande **more system:running-config**, vous pouvez copier et coller la clé partagée chiffrée avec succès. **Remarque** Le secret partagé **failover key** s'affiche comme ***** dans la sortie **show running-config**; cette clé masquée ne peut pas être copiée. Il n'y a eu aucune modification d'ASDM.
Ajout de la prise en charge d'IPv6 pour le basculement.	8.2(2)	Nous avons modifié les écrans suivants : Configuration > Device Management (Gestion des périphériques) > High Availability (Haute disponibilité) > Failover (Basculement) > Setup (Configuration) Configuration > Device Management (Gestion des périphériques) > High Availability (Haute disponibilité) > Failover (Basculement) > Interfaces
Modifiez la préférence de l'unité de groupe de basculement lors du démarrage « simultané ».	9.0(1)	Les versions logicielles antérieures permettaient un démarrage « simultané » de sorte que les groupes de basculement ne devaient pas exiger que la commande **preempt** devienne active sur l'unité préférée. Cependant, cette fonctionnalité a maintenant été modifiée, de sorte que les deux groupes de basculement deviennent actifs sur la première unité de démarrage.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge des tunnels IPsec LAN à LAN pour chiffrer les communications de liaison de basculement et d'état	9.1(2)	Au lieu d'utiliser le chiffrement propriétaire pour la clé de basculement, vous pouvez désormais utiliser un tunnel IPsec LAN à LAN pour le chiffrement de la liaison de basculement et d'état. **Remarque** Les tunnels de basculement LAN à LAN ne sont pas pris en compte dans la licence IPsec (autre VPN). Nous avons modifié l'écran suivant : **Configuration > Device Management (Gestion des périphériques) > High Availability (Haute disponibilité) > Failover (Basculement) > Setup (Configuration)**.
Désactiver la surveillance de l'intégrité d'un module matériel	9.3(1)	Par défaut, l'ASA surveille l'intégrité d'un module matériel installé tel que le module ASA FirePOWER. Si vous ne souhaitez pas qu'une défaillance du module matériel déclenche le basculement, vous pouvez désactiver la surveillance du module. Nous avons modifié l'écran suivant : **Configuration > Device Management (Gestion des périphériques) > High Availability and Scalability (Haute disponibilité et évolutivité) > Failover (Basculement) > Interfaces**.
Verrouiller les modifications de configuration sur l'unité de veille ou le contexte de veille dans une paire de basculement	9.3(2)	Vous pouvez désormais verrouiller les modifications de configuration sur l'unité de veille (basculement actif/veille) ou sur le contexte de veille (basculement actif/actif) afin de ne pas pouvoir apporter des modifications sur l'unité de veille en dehors de la synchronisation normale de la configuration. Nous avons modifié l'écran suivant : **Configuration > Device Management (Gestion des périphériques) > High Availability and Scalability (Haute disponibilité et évolutivité) > Failover (Basculement) > Setup (Configuration)**.
Activer l'utilisation de l'interface de gestion Management 1/1 comme liaison de basculement sur l'ASA 5506H	9.5(1)	Sur l'ASA 5506H uniquement, vous pouvez maintenant configurer l'interface de gestion Management 1/1 comme liaison de basculement. Cette fonctionnalité vous permet d'utiliser toutes les autres interfaces du périphérique comme interfaces de données. Notez que si vous utilisez cette fonctionnalité, vous ne pouvez pas utiliser le module ASA Firepower, ce qui nécessite que l'interface de gestion Management 1/1 reste une interface de gestion normale. Nous avons modifié l'écran suivant : **Configuration > Device Management (Gestion des périphériques) > High Availability and Scalability (Haute disponibilité et évolutivité) > Failover (Basculement) > Setup (Configuration)**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Les améliorations de la NAT de classe opérateur sont désormais prises en charge dans le basculement et la mise en grappe d'ASA	9.5(2)	Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois (Voir RFC 6888). Cette fonctionnalité est désormais prise en charge dans les déploiements de basculement et de grappe ASA. Nous n'avons pas modifié d'écrans.
Temps de synchronisation amélioré pour les ACL dynamiques de Secure Client (services client sécurisés) lors de l'utilisation du basculement actif/veille	9.6(2)	Lorsque vous utilisez Secure Client (services client sécurisés) sur une paire de basculement, le temps de synchronisation des ACL dynamiques (dACLs) associées avec l'unité de veille est maintenant amélioré. Auparavant, avec de grandes dACLs, le temps de synchronisation pouvait prendre des heures pendant lesquelles l'unité de veille était occupée à synchroniser au lieu de fournir une sauvegarde à haute disponibilité. Nous n'avons pas modifié d'écrans.
Basculement avec état pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple	9.6(2)	Le basculement avec état est maintenant pris en charge pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple. Nous n'avons pas modifié d'écrans.
L'interrogation de la surveillance de l'état de la liaison de l'interface pour le basculement est désormais configurable pour une détection plus rapide	9.7(1)	Par défaut, chaque ASA d'une paire de basculement vérifie l'état de liaison de ses interfaces toutes les 500 ms. Vous pouvez maintenant configurer l'intervalle entre interrogations, entre 300 ms et 799 ms; par exemple, si vous définissez le délai d'interrogation à 300 ms, l'ASA peut détecter une défaillance d'interface et déclencher le basculement plus rapidement. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **Failover (Basculement)** > **Criteria (Critères)**
Prise en charge de la détection de transfert bidirectionnel (BFD) pour la surveillance de l'intégrité du basculement actif/veille sur les périphériques Firepower 9300 et 4100.	9.7(1)	Vous pouvez activer la détection de transfert bidirectionnel (BFD) pour la vérification de l'intégrité du basculement entre deux unités d'une paire active/veille sur les périphériques Firepower 9300 et 4100. L'utilisation de la BFD pour la vérification de l'intégrité est plus fiable que la méthode de vérification de l'intégrité par défaut et utilise moins de CPU. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **Failover (Basculement)** > **Setup (Configuration)**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Désactiver le délai de basculement	9.15(1)	Lorsque vous utilisez des groupes de ponts ou DAD IPv6, lorsqu'un basculement se produit, la nouvelle unité active attend jusqu'à 3 000 ms que l'unité de veille termine les tâches de mise en réseau et passe à l'état de veille. Ensuite, l'unité active peut commencer à transmettre du trafic. Pour éviter ce délai, vous pouvez désactiver le délai d'attente afin que l'unité active commence à transmettre le trafic avant l'unité de veille. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **Failover (Basculement)** > **Enable switchover waiting for peer state (Activer le basculement en attente de l'état des pairs)**
Fonction d'optimisation Config-Sync pour un appairage haute disponibilité	9.18(1)	La fonctionnalité d'optimisation de la synchronisation de la configuration permet de comparer la configuration de l'unité qui rejoint l'unité et de l'unité active en échangeant des valeurs de hachage de configuration. Si le hachage calculé sur les unités actives et en cours de jonction correspond, l'unité à joindre ignore la configuration de synchronisation complète et rejoint la haute disponibilité. Cette fonctionnalité accélère l'appairage à haute disponibilité et réduit la fenêtre de maintenance ainsi que le temps de mise à niveau.



CHAPITRE 11

Basculement pour la haute disponibilité dans le nuage public

Ce chapitre décrit comment configurer le basculement actif/de secours pour atteindre la haute disponibilité de l'ASA virtuel dans un environnement de nuage public, comme Microsoft Azure.

- À propos du basculement dans le nuage public, à la page 345
- Licences pour le basculement dans le nuage public, à la page 350
- Valeurs par défaut pour le basculement dans le nuage public, à la page 350
- À propos de l'ASA virtuel à haute disponibilité dans Microsoft Azure, à la page 351
- Configurer le basculement actif/de secours, à la page 354
- Configurer les paramètres de basculement facultatifs, à la page 357
- Gérer le basculement dans le nuage public, à la page 358
- Superviser le basculement dans le nuage public, à la page 360
- Historique de basculement dans le nuage public, à la page 361

À propos du basculement dans le nuage public

Pour assurer la redondance, vous pouvez déployer l'ASA virtuel dans un environnement de nuage public dans une configuration active/de secours à haute accessibilité (HA). La haute accessibilité dans le nuage public met en œuvre une solution active/de secours sans état qui permet, en cas de défaillance de l'ASA virtuel actif, de déclencher un basculement automatique du système vers l'ASA virtuel de secours.

La liste suivante décrit les composants principaux de la solution de nuage public à haute disponibilité :

- **ASA virtuel actif** : l'ASA virtuel dans la paire à haute disponibilité qui est configuré pour gérer le trafic de pare-feu pour les homologues à haute disponibilité.
- **ASA virtuel en veille** : l'ASA virtuel dans la paire à haute disponibilité qui ne gère pas le trafic du pare-feu et prend le relais comme ASA virtuel actif en cas de défaillance d'un ASA virtuel actif. Il est appelé sauvegarde plutôt que de secours, car il ne prend pas l'identité de son homologue en cas de basculement.
- **Agent à haute disponibilité** : un processus allégé qui s'exécute sur l'ASA virtuel et détermine le rôle de haute disponibilité (actif/sauvegarde) d'un ASA virtuel, détecte les défaillances de son homologue à haute disponibilité et effectue les actions en fonction de son rôle de haute disponibilité.

Sur l'ASA physique et l'ASA virtuel en nuage non public, le système gère les conditions de basculement à l'aide de demandes ARP gratuites, dans lesquelles l'ASA de secours envoie une requête ARP gratuite indiquant qu'il est désormais associé aux adresses IP et MAC actives. La plupart des environnements de nuage public n'autorisent pas le trafic de diffusion de cette nature. Pour cette raison, une configuration à haute disponibilité dans le nuage public nécessite le redémarrage des connexions permanentes lors du basculement.

L'intégrité de l'unité active est surveillée par l'unité de secours pour déterminer si des conditions de basculement spécifiques sont remplies. Si ces conditions sont remplies, le basculement se produit. Le délai de basculement peut varier de quelques secondes à plus d'une minute selon la réactivité de l'infrastructure de nuage public.

À propos du basculement actif/de secours

Dans le basculement actif/sauvegarde, une unité est l'unité active. Elle transmet le trafic. L'unité de sauvegarde ne transmet pas activement le trafic et n'échange aucune information de configuration avec l'unité active. Le basculement actif/de sauvegarde vous permet d'utiliser un périphérique ASA virtuel de sauvegarde pour reprendre les fonctionnalités d'une unité en panne. Lorsque l'unité active tombe en panne, elle passe à l'état de sauvegarde pendant que l'unité de sauvegarde passe à l'état actif.

Rôles principal/secondaire et état actif/de secours

Lors de la configuration du basculement actif/de sauvegarde, vous configurez une unité comme principale et l'autre comme secondaire. À ce stade, les deux unités agissent comme deux périphériques distincts pour la configuration des périphériques et des politiques, ainsi que pour les événements, les tableaux de bord, les rapports et la surveillance de l'intégrité.

Les principales différences entre les deux unités d'une paire de basculement dépendent de l'unité active et de l'unité de sauvegarde, à savoir l'unité qui transmet activement le trafic. Bien que les deux unités soient capables de transmettre du trafic, seule l'unité principale répond aux sondes de l'équilibreur de charges et programme toutes les routes configurées pour l'utiliser comme destination de routage. La fonction principale de l'unité de sauvegarde est de surveiller l'intégrité de l'unité principale. L'unité principale devient toujours l'unité active si les deux unités démarrent en même temps (et ont le même état de fonctionnement opérationnel).

Connexion de basculement

L'ASA virtuel de secours surveille l'intégrité de l'ASA virtuel actif à l'aide d'une connexion de basculement établie sur TCP :

- L'ASA virtuel actif agit comme un serveur de connexion en ouvrant un *port d'écoute*.
- L'ASA virtuel de secours se connecte à l'ASA virtuel actif à l'aide du *port de connexion*.
- En général, le *port d'écoute* et le *port de connexion* sont identiques, sauf si votre configuration requiert une traduction d'adresses réseau entre les unités ASA virtuel.

L'état de la connexion de basculement détecte la défaillance de l'ASA virtuelactif. Lorsque l'ASA virtuel de secours voit la connexion de basculement établie, il considère l'ASA virtuel actif comme *ayant échoué*. De même, si l'ASA virtuel de secours ne reçoit pas de réponse à un message keepalive envoyé à l'unité active, il considère l'ASA virtuel actif comme *ayant échoué*.

Thèmes connexes

Messages de sondage et Hello

L'ASA virtuel de secours envoie des messages Hello via la connexion de basculement à l'ASA virtuel actif et attend une réponse Hello en retour. La synchronisation des messages utilise un intervalle entre les interrogations, la période entre la réception d'une réponse Hello par l'unité ASA virtuel de secours et l'envoi du message Hello suivant. La réception de la réponse est imposée par un délai d'expiration de réception, appelé délai de rétention. Si la réception de la réponse Hello expire, l'ASA virtuel actif est considéré comme ayant échoué.

Les intervalles d'interrogation et de délai de rétention sont des paramètres configurables; voir Configurer le basculement actif/de secours, à la page 354.

Détermination de l'unité active au démarrage

L'unité active est déterminée par les éléments suivants :

- Si une unité démarre et détecte un homologue qui fonctionne déjà comme actif, elle devient l'unité de sauvegarde.
- Si une unité démarre et ne détecte pas d'homologue, elle devient l'unité active.
- Si les deux unités démarrent simultanément, l'unité principale devient l'unité active et l'unité secondaire devient l'unité de sauvegarde.

Événements de basculement

Dans le cas d'un basculement actif/de secours, le basculement se produit de manière unitaire. Le tableau suivant présente l'action de basculement pour chaque défaillance. Pour chaque défaillance, le tableau indique la politique de basculement (basculement ou absence de basculement), l'action prise par l'unité active, l'action entreprise par l'unité de sauvegarde, et toute remarque spéciale sur la condition et les actions de basculement.

Tableau 21 : Événements de basculement

Défaillance	Politique	Action active	Action de sauvegarde	Notes
L'unité de sauvegarde voit une connexion de basculement se fermer	Basculement	S.O.	Devenir active Marquer l'unité active comme défaillante	Il s'agit du scénario de basculement standard.
L'unité active voit une connexion de basculement se fermer	Aucun basculement	Marquer la sauvegarde comme ayant échoué	S.O.	Le basculement vers une unité inactive ne doit jamais se produire.

Défaillance	Politique	Action active	Action de sauvegarde	Notes
L'unité active voit un délai d'expiration TCP sur la liaison de basculement	Aucun basculement	Marquer la sauvegarde comme ayant échoué	Aucune action	Le basculement ne doit pas se produire si l'unité active ne reçoit pas de réponse de l'unité de sauvegarde.
L'unité de sauvegarde voit un délai d'expiration TCP sur la liaison de basculement	Basculement	S.O.	Devenir active Marquer l'unité active comme défaillante Essayer d'envoyer la commande de basculement à l'unité active	L'unité de sauvegarde suppose que l'unité active n'est pas en mesure de continuer à fonctionner et prend le relais. Si l'unité active est toujours opérationnelle, mais n'envoie pas de réponse à temps, l'unité de sauvegarde envoie la commande de basculement à l'unité active.
Échec de l'authentification de l'unité active	Aucun basculement	Aucune action	Aucune action	Comme l'unité de sauvegarde modifie les tables de routage, c'est la seule unité qui doit être authentifiée auprès d'Azure. Peu importe si l'unité active est authentifiée auprès d'Azure ou non.
Échec de l'authentification de l'unité de sauvegarde	Aucun basculement	Marquer la sauvegarde comme non authentifiée	Aucune action	Le basculement ne peut pas se produire si l'unité de sauvegarde n'est pas authentifiée auprès d'Azure.
L'unité active lance le basculement intentionnel	Basculement	Devenir une sauvegarde	Devenir active	L'unité active lance le basculement et ferme la connexion de liaison de basculement. L'unité de sauvegarde voit la connexion se terminer et devient l'unité active.
L'unité de sauvegarde lance le basculement intentionnel	Basculement	Devenir une sauvegarde	Devenir active	L'unité de sauvegarde lance le basculement en envoyant un message de basculement à l'unité active. Lorsque l'unité active voit le message, elle ferme la connexion et devient l'unité de sauvegarde. L'unité de sauvegarde voit la connexion se terminer et devient l'unité active.

Défaillance	Politique	Action active	Action de sauvegarde	Notes
L'unité précédemment active récupère	Aucun basculement	Devenir une sauvegarde	Marquer le partenaire comme sauvegarde	Le basculement ne doit pas se produire, sauf si cela est absolument nécessaire.
L'unité active voit le message de basculement de l'unité de sauvegarde	Basculement	Devenir une sauvegarde	Devenir active	Peut se produire si un basculement manuel a été lancé par un utilisateur, ou si l'unité de sauvegarde a vu le délai d'expiration TCP, mais l'unité active est en mesure de recevoir des messages de l'unité de sauvegarde.

Lignes directrices et limites relatives à la licence

Cette section comprend les lignes directrices et les limites de cette fonctionnalité.

ASA virtuel Basculement pour la haute disponibilité dans le nuage public

Pour assurer la redondance, vous pouvez déployer l'ASA virtuel dans un environnement de nuage public dans une configuration active/de secours à haute accessibilité (HA).

- Pris en charge uniquement dans le cloud public Microsoft Azure ; lors de la configuration de la machine virtuelle ASA virtuel, le nombre maximal de vCPU pris en charge est de 16 et la mémoire maximale prise en charge est de 64 Go de RAM. Consultez le Guide de démarrage d'ASA virtuel pour obtenir la liste complète des instances prises en charge.
- Met en œuvre une solution active/de secours sans état qui permet, en cas de défaillance de l'ASA virtuel actif, de déclencher un basculement automatique du système vers l'ASA virtuel de secours.

Restrictions

- Le basculement se fait de l'ordre des secondes plutôt que des millisecondes.
- La détermination du rôle à haute disponibilité et la capacité de participer en tant qu'unité à haute disponibilité dépendent de la connectivité TCP entre les homologues à haute disponibilité et entre une unité à haute disponibilité et l'infrastructure Azure. Il existe plusieurs situations où un ASA virtuel ne pourra pas participer en tant qu'unité à haute disponibilité :
  - L'incapacité à établir une connexion de basculement avec son homologue à haute disponibilité.
  - L'incapacité à récupérer un jeton d'authentification à partir d'Azure.
  - L'incapacité à s'authentifier auprès d'Azure.
- Il n'y a pas de synchronisation de la configuration de l'unité active avec l'unité de sauvegarde. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.
- Limites de la table de routage de basculement

En ce qui concerne les tables de routage pour la haute disponibilité dans le nuage public :

- Vous pouvez configurer un maximum de 16 tables de routage.
- Dans une table de routage, vous pouvez configurer un maximum de 64 routes.

Dans chaque cas, le système vous alerte lorsque vous avez atteint la limite, en vous recommandant de supprimer une table de routage ou une route et de réessayer.

- ASDM n'est pas pris en charge.
- Aucune prise en charge du VPN d'accès à distance IPSec.

Remarque Consultez le guide de démarrage rapide de Cisco Adaptive Security Virtual Appliance (ASAv) pour obtenir des renseignements sur les topologies VPN prises en charge dans le nuage public.

- Les instances de machine virtuelle ASA virtuel doivent se trouver dans le même ensemble de disponibilité. Si vous êtes un utilisateur ASA virtuel actuel dans Azure, vous ne pourrez pas effectuer de mise à niveau vers la haute disponibilité à partir d'un déploiement existant. Vous devez supprimer votre instance et déployer l'offre ASA virtuel 4 NIC à haute disponibilité depuis le Marché Azure.

Licences pour le basculement dans le nuage public

L'ASA virtuel utilise les licences logicielles Cisco Smart. Une licence Smart est requise pour le fonctionnement normal. Chaque ASA virtuel doit recevoir une licence indépendante avec une licence de plateforme ASA virtuel. Jusqu'à ce que vous installiez une licence, le débit est limité à 100 kbit/s. Vous pouvez donc effectuer des tests de connectivité préalables. Consultez la page Licences de fonctionnalités de la gamme Cisco ASA pour connaître les exigences de licence précises pour l'ASA virtuel.

Valeurs par défaut pour le basculement dans le nuage public

Par défaut, la politique de basculement comprend les éléments suivants :

- Basculement sans état uniquement.
- Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.
- Le numéro de port de contrôle de basculement TCP est 44442.
- Le numéro de port de la sonde d'intégrité de l'équilibreur de charges Azure est 44441.
- Le délai d'interrogation de l'unité est de 5 secondes.
- Le délai de rétention de l'unité est de 15 secondes.
- L'ASA virtuel répond aux sondes d'intégrité sur l'interface principale (Management 0/0).

- L'authentification ASA virtuel avec le principal de service Azure est effectuée sur l'interface principale (Management 0/0).

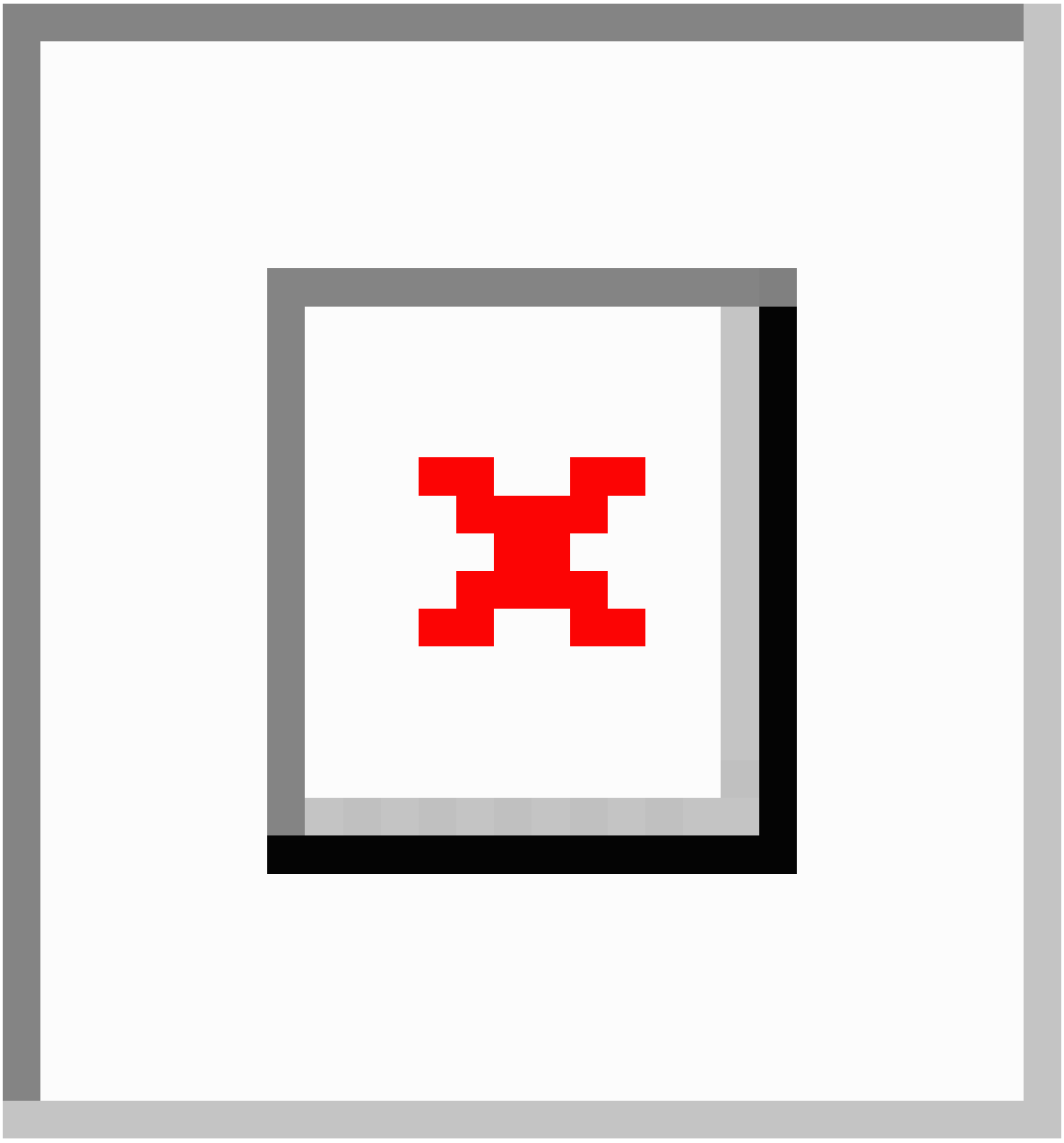
Remarque Consultez Configurer les paramètres de basculement facultatifs, à la page 357 pour connaître les options permettant de modifier le numéro de port de basculement, le numéro de port de la sonde d'intégrité, les délais d'interrogation et l'interface principale.

À propos de l'ASA virtuel à haute disponibilité dans Microsoft Azure

La figure suivante présente une vue d'ensemble d'un déploiement de l'ASA virtuel à haute disponibilité dans Azure. Une charge de travail protégée se trouve derrière deux instances ASA virtuel dans une configuration de basculement actif/de sauvegarde. Un équilibreur de charges Azure sonde les deux unités ASA virtuel à l'aide d'une liaison TCP tridirectionnelle. L'ASA virtuel actif termine l'établissement de la liaison tridirectionnelle indiquant qu'il est intègre, tandis que l'ASA virtuel de sauvegarde ne répond pas intentionnellement. En ne répondant pas à l'équilibreur de charges, l'ASA virtuel de sauvegarde semble non intègre à l'équilibreur de charges, qui à son tour, ne lui envoie pas de trafic.

Lors du basculement, l'ASA virtuel actif arrête de répondre aux sondes de l'équilibreur de charges et l'ASA virtuel de sauvegarde commence à répondre, ce qui fait que toutes les nouvelles connexions sont envoyées à l'ASA virtuel de sauvegarde. L'ASA virtuel de sauvegarde envoie des demandes API à la structure Azure pour modifier la table de routage, redirigeant ainsi le trafic de l'unité active vers l'unité de sauvegarde. À ce stade, l'ASA virtuel de sauvegarde devient l'unité active et l'unité active devient l'unité de sauvegarde ou est hors ligne, selon la raison du basculement.

Illustration 55 : Déploiement de l'ASA virtuel à haute disponibilité dans Azure



Pour pouvoir passer automatiquement des appels d'API pour modifier les tables de routage Azure, les unités ASA virtuel à haute disponibilité doivent disposer de renseignements d'authentification Azure Active Directory. Azure utilise le concept de principal de service qui, en termes simples, est un compte de service. Un principal de service vous permet de provisionner un compte avec seulement les autorisations et la portée nécessaires pour exécuter une tâche dans un ensemble prédéfini de ressources Azure.

Il y a deux étapes pour permettre à votre déploiement ASA virtuel à haute disponibilité de gérer votre abonnement Azure à l'aide d'un principal de service :

1. Créez une application Azure Active Directory et un principal de service; voir À propos du principal de service Azure, à la page 353.

2. Configurez les instances ASA virtuel pour s'authentifier auprès d'Azure à l'aide d'un principal de service; voir Configurer le basculement actif/de secours, à la page 354.

Thèmes connexes

Consultez la documentation d'Azure pour en savoir plus sur l'équilibreur de charges.

À propos du principal de service Azure

Lorsque vous avez une application qui a besoin d'accéder aux ressources d'Azure ou de les modifier, telles que des tables de routage, vous devez configurer une application Azure Active Directory (AD) et lui attribuer les autorisations requises. Il est préférable d'exécuter cette approche sous vos propres informations d'authentification, car :

- Vous pouvez attribuer des autorisations à l'identité de l'application qui sont différentes de vos propres autorisations. En règle générale, ces autorisations se limitent à ce que doit faire l'application.
- Vous n'avez pas besoin de modifier les informations d'authentification de l'application si vos responsabilités changent.
- Vous pouvez utiliser un certificat pour automatiser l'authentification lors de l'exécution d'un script sans surveillance.

Lorsque vous enregistrez une application Azure AD dans le portail Azure, deux objets sont créés dans votre détenteur Azure AD : un objet d'application et un objet de principal de service.

- **Application object** (Objet d'application) : une application Azure AD est définie par son seul et unique objet d'application, qui réside dans le détenteur Azure AD où l'application a été enregistrée, appelé détenteur « local » de l'application.
- **Service principal object** (Objet de principal de service) : l'objet de principal de service définit la politique et les autorisations pour l'utilisation d'une application dans un détenteur spécifique, fournissant la base d'un principal de sécurité pour représenter l'application lors de l'exécution.

Azure fournit des instructions sur la création d'une application et d'un principal de service Azure AD dans la *documentation d'Azure Resource Manager*. Consultez les rubriques suivantes pour obtenir des instructions complètes :

- Utiliser le portail pour créer une application et un principal de service Azure Active Directory qui peuvent accéder aux ressources
- Utiliser Azure PowerShell pour créer un principal de service pour accéder à la ressource

Remarque Après avoir configuré le principal de service, procurez-vous le **Directory ID** (ID de répertoire), l'**Application ID** (ID d'application) et la **Secret key** (Clé secrète). Ces éléments sont requis pour configurer les informations d'authentification Azure; voir Configurer le basculement actif/de secours, à la page 354.

Exigences de configuration pour ASA virtuel haute disponibilité dans Azure

Pour déployer une configuration similaire à celle décrite dans #unique_474 unique_474_Connect_42_fig_cgx_dlh_h1b, vous avez besoin des éléments suivants :

- Renseignements d'authentification Azure (voir À propos du principal de service Azure, à la page 353) :
  - ID de répertoire
  - ID d'application
  - Clé secrète
- Renseignements sur les routes Azure (voir Configurer les tableaux de routage Azure, à la page 357) :
  - ID d'abonnement Azure
  - Groupe de ressources de la table de routage
  - Noms de tables
  - Préfixe d'adresse
  - Adresse du saut suivant
- Configuration de l'ASA (voir Configurer le basculement actif/de secours, à la page 354, Valeurs par défaut pour le basculement dans le nuage public, à la page 350) :
  - Adresses IP actives ou de secours
  - Port de communication de l'agent à haute disponibilité
  - Port de sonde de l'équilibreur de charges
  - Intervalles entre interrogations



Remarque Configurez les paramètres de basculement de base sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.

Configurer le basculement actif/de secours

Pour configurer le basculement actif/de secours, configurez les paramètres de basculement de base sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.

Avant de commencer

- Déployez votre paire ASA virtuel à haute disponibilité dans un ensemble de disponibilité Azure.

- Ayez les renseignements sur votre environnement Azure à disposition, y compris votre ID d'abonnement Azure et vos informations d'authentification Azure pour le principal du service.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **Failover (Basculement)**.

Étape 2 Sous l'onglet **Cloud** (Nuage), cochez la case **Unit** (Unité) pour développer les options déroulantes **Failover Unit** (Unité de basculement).

Étape 3 Dans le menu déroulant **Failover Unit** (Unité de basculement), choisissez **primary** (principale).

L'unité principale assumera le rôle de haute disponibilité actif lorsque les deux unités de haute disponibilité seront déployées en même temps.

Étape 4 (Facultatif) Cochez la case **Port** pour développer les champs **Control** (Contrôle) et **Probe** (Sonde).

a) Saisissez un port de contrôle TCP valide dans le champ **Control** (Contrôle); ou conservez la valeur par défaut, le port 44442.

Le port de contrôle établit la connexion de basculement TCP établie entre l'ASA virtuel actif et l'ASA virtuel de secours.

b) Saisissez un port de sonde TCP valide dans le champ **Probe** (Sonde); ou conservez la valeur par défaut, le port 44441.

Le port de sonde est le port TCP utilisé comme port de destination pour les sondes de l'équilibreur de charges Azure.

Étape 5 (Facultatif) Cochez la case **Time** (Heure) pour développer les champs **Poll Time** (Délai d'interrogation) et **Hold Time** (Délai de rétention).

a) Saisissez une durée valide (en secondes) dans le champ **Poll Time** (Délai d'interrogation); ou conservez la valeur par défaut, 5 secondes.

La plage du délai d'interrogation est comprise entre 1 et 15 secondes. Grâce à un délai d'interrogation plus court, l'ASA peut détecter les défaillances et déclencher le basculement plus rapidement. Cependant, une détection plus rapide peut entraîner des basculements inutiles lorsque le réseau est temporairement congestionné.

b) Saisissez une durée valide (en secondes) dans le champ **Hold Time** (Délai de rétention); ou conservez la valeur par défaut, 15 secondes.

Le délai de rétention détermine le délai entre le moment où un paquet Hello est manqué et le moment où l'unité est marquée comme défaillante. La plage du délai de rétention est comprise entre 3 et 60 secondes. Vous ne pouvez pas saisir une valeur de délai de rétention inférieure à 3 fois le délai d'interrogation de l'unité.

Étape 6 Cochez la case **Peer** (Homologue) pour développer les champs **Peer IP-Address** (Adresse IP homologue) et **Peer Port** (Port homologue).

a) Saisissez l'adresse IP utilisée pour établir une connexion de contrôle de basculement TCP avec l'homologue à haute disponibilité dans le champ **Peer IP-Address** (Adresse IP homologue).

b) (Facultatif) Saisissez un port de contrôle TCP valide dans le champ **Peer Port** (Port homologue); ou conservez la valeur par défaut, port 44442.

Le port homologue établit la connexion de basculement TCP établie entre l'ASA virtuel actif et l'ASA virtuel de secours.

Étape 7 Cochez la case **Authentication** (Authentification) pour développer les champs **Application-id** (ID d'application), **Directory-id** (ID de répertoire) et **Key** (Clé).

Vous pouvez configurer les informations d'authentification pour un principal de service Azure qui permet à vos homologues ASA virtuel à haute disponibilité d'accéder aux ressources d'Azure et de les modifier, telles que les tables de routage. Les principaux de service vous permettent de provisionner un compte Azure qui possède les autorisations minimales pour effectuer une tâche dans un ensemble prédéfini de ressources Azure. Dans le cas de l'ASA virtuel à haute disponibilité, il est limité aux autorisations nécessaires pour modifier les routes définies par l'utilisateur; voir À propos du principal de service Azure, à la page 353.

a) Saisissez l'ID d'application Azure pour le principal de service Azure dans le champ **Application-id** (ID d'application).

Vous avez besoin de cet ID d'application lorsque vous demandez une clé d'accès auprès de l'infrastructure Azure.

b) Saisissez l'ID de répertoire Azure pour le principal du service Azure dans le champ **Directory-id** (ID de répertoire).

Vous avez besoin de cet ID de répertoire lorsque vous demandez une clé d'accès auprès de l'infrastructure Azure.

c) Saisissez la clé secrète Azure pour le principal du service Azure dans le champ **Key** (Clé).

Vous avez besoin de cette clé secrète lorsque vous demandez une clé d'accès auprès de l'infrastructure Azure. Si le champ **Encrypt** (Chiffrer) est coché, la clé secrète est chiffrée dans la configuration en cours d'exécution.

Étape 8 Cochez la case **Subscription** (Abonnement) pour développer le champ **Sub-id** (ID d'abonnement).

Il s'agit de l'ID d'abonnement pour le compte auquel les tables de routage qui nécessitent une mise à jour appartiennent.

Étape 9 Cochez la case **Enable Cloud Failover** (Activer le basculement dans le nuage).

Étape 10 Cliquez sur **Apply** (Appliquer).

Le basculement n'est pas activé jusqu'à ce que vous appliquiez vos modifications au périphérique.

Étape 11 Si vous savez que l'unité secondaire n'est pas encore activée, connectez-vous à l'ASA virtuel secondaire à partir de **Device List** (Liste des périphériques), ou démarrez une nouvelle session ASDM en utilisant l'adresse IP de l'ASA virtuel : **https***://asa_ip_address/***admin**.

Étape 12 Répétez les étapes 1 à 10 pour configurer le basculement actif/de sauvegarde sur l'unité secondaire.

Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.

Le basculement n'est pas activé jusqu'à ce que vous appliquiez vos modifications au périphérique.

Prochaine étape

Configurez les paramètres supplémentaires au besoin :

- Configurez les renseignements sur les routes Azure; voir Configurer les tableaux de routage Azure, à la page 357.

Configurer les paramètres de basculement facultatifs

Vous pouvez personnaliser les paramètres de basculement selon vos besoins.

Configurer les tableaux de routage Azure

La configuration de la table de routage comprend des renseignements sur les routes définies par l'utilisateur Azure qui doivent être mises à jour lorsque l'ASA virtuel assume le rôle actif. Lors du basculement, vous souhaitez diriger des routes internes vers l'unité active, qui utilise les renseignements de la table de routage configurée pour diriger automatiquement les routes vers elle-même.

Remarque Vous devez configurer tous les renseignements de la table de routage Azure sur les unités actives et de sauvegarde.

Avant de commencer

- Configurez ces paramètres sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire.
- Ayez les renseignements sur votre environnement Azure à disposition, y compris votre ID d'abonnement Azure et vos informations d'authentification Azure pour le principal du service.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **Failover (Basculement)**.

Étape 2 Cliquez sur l'onglet **Route-Table**, puis sur **Add** (Ajouter).

a) Dans le champ **Route Table Name** (Nom de la table de routage), saisissez un nom pour la table de routage.

Vous pouvez configurer jusqu'à 16 tables de routage. Par ailleurs, vous pouvez modifier ou supprimer des entrées de la liste de la table de routage.

b) (Facultatif) Dans le champ **Sub-id**, saisissez un ID d'abonnement Azure.

Vous pouvez mettre à jour des routes définies par l'utilisateur dans plusieurs abonnements Azure en spécifiant l'ID d'abonnement Azure correspondant ici. Si vous saisissez le **Route Table Name** (Nom de la table de routage) sans spécifier d'ID d'abonnement Azure, le paramètre global est utilisé.

Remarque Vous saisissez l'ID d'abonnement Azure lorsque vous configurez le basculement actif/de secours à partir de **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et d'évolutivité)** > **Failover (Basculement)**; voir Configurer le basculement actif/de secours, à la page 354.

Étape 3 Cliquez sur **Route-Table-Mode** (Mode de table de routage). Vous pouvez ajouter, modifier ou supprimer des entrées de routage dans les tables de routage.

Étape 4 Cliquez sur **Add** (ajouter).

Saisissez les valeurs suivantes pour les routes définies par l'utilisateur Azure :

a) Dans la liste déroulante **Route Table** (Table de routage), choisissez une table de routage.
b) Dans le champ **Azure Resource Group** (Groupe de ressources Azure), saisissez le nom du groupe de ressources Azure qui contient la table de routage Azure.
c) Dans le champ **Route Name** (Nom de la route), saisissez un nom unique pour la route.
d) Dans le champ **Prefix Address/Mask** (Adresse de préfixe/masque), saisissez le préfixe de l'adresse IP, en notation CIDR.
e) Dans le champ **Next Hop Address** (Adresse de saut suivant), saisissez l'adresse du saut suivant. Voici une adresse IP d'interface sur l'ASA virtuel.

Remarque Vous pouvez configurer jusqu'à 64 routes.

Étape 5 Cliquez sur **Apply** pour enregistrer vos modifications.

Gérer le basculement dans le nuage public

Cette section décrit comment gérer les unités Basculement dans le nuage après avoir activé le basculement, y compris comment forcer le basculement d'une unité à une autre.

Forcer le basculement

Pour forcer l'unité en veille à devenir active, exécutez la commande suivante.

Avant de commencer

Utilisez cette commande dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Failover (Basculement)** > **Status (État)**

Étape 2 Pour forcer le basculement au niveau de l'unité, cliquez sur l'un des boutons suivants :

- Cliquez sur **Make Active** (Rendre actif) pour faire de cette unité l'unité *active*.
- Cliquez sur **Make Standby** (Mettre en veille) pour faire de cette unité l'unité *en veille*.

Mettre à jour les routes

Si l'état des routes dans Azure est incohérent avec l'ASA virtuel dans le rôle *actif*, vous pouvez forcer les mises à jour de routes sur l'ASA virtuel :

Avant de commencer

Utilisez cette commande dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Failover (Basculement)** > **Status (État)**

Étape 2 Cliquez sur **Update Route** (Mettre à jour la route).

Cette commande est uniquement valide sur l'ASA virtuel dans le rôle *actif*. Si l'authentification échoue, la sortie sera `Route changes failed`.

Valider l'authentification Azure

Pour un déploiement réussi de l'ASA virtuel à haute disponibilité dans Azure, la configuration du principal de service doit être complète et précise. Sans l'autorisation Azure appropriée, les unités ASA virtuel ne pourront pas accéder aux ressources pour gérer le basculement et effectuer des mises à jour de routage. Vous pouvez tester votre configuration de basculement pour détecter les erreurs liées aux éléments suivants de votre principal de service Azure :

- ID de répertoire
- ID d'application
- Clé d'authentification

Avant de commencer

Utilisez cette commande dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Failover (Basculement)** > **Status (État)**

Étape 2 Cliquez sur **Test Authentication** (Tester l'authentification).

Si l'authentification échoue, la sortie de la commande sera `Authentication Failed` (Échec d'authentification).

Si l'ID de répertoire ou l'ID d'application n'est pas configuré correctement, Azure ne reconnaîtra pas la ressource mentionnée dans la demande REST pour obtenir un jeton d'authentification. L'historique des événements pour cette entrée de condition indiquera :

```
Error Connection - Unexpected status in response to access token request: Bad Request
```

Si l'ID de répertoire ou l'ID d'application sont corrects, mais que la clé d'authentification n'est pas configurée correctement, Azure n'accordera pas l'autorisation de générer le jeton d'authentification. L'historique des événements pour cette entrée de condition indiquera :

```
Error Connection - Unexpected status in response to access token request: Unauthorized
```

Superviser le basculement dans le nuage public

Cette section explique comment superviser l'état du basculement.

État de basculement

Remarque Après un événement de basculement, vous devez soit lancer à nouveau ASDM, soit passer à un autre périphérique dans le volet Devices (Périphériques), puis revenir à l'ASA d'origine pour continuer à superviser le périphérique. Cette action est nécessaire, car la connexion de surveillance ne sera pas rétablie lorsque ASDM est déconnecté, puis reconnecté au périphérique.

- Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Failover (Basculement)** > **Status (État)** et cliquez sur **Failover Status** (État de basculement) pour surveiller l'état du basculement actif/de secours.
- Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Failover (Basculement)** > **History (Historique)** pour afficher l'historique des événements de basculement avec un horodatage, un niveau de gravité, un type d'événement et un texte d'événement.

Messages de basculement

Messages de journal système de basculement

L'ASA émet un certain nombre de messages de journal système liés au basculement au niveau de priorité 2, ce qui indique une condition critique. Pour afficher ces messages, consultez le guide des messages du journal système. Les messages de journal système sont compris entre 1045xx et 1055xx.

Remarque Pendant le basculement, l'ASA s'éteint de manière logique, puis affiche des interfaces, générant des messages de journal système. Il s'agit d'une activité normale.

Voici des exemples de journaux système générés lors d'un basculement :

```
%ASA-3-105509: (Primary) Error sending Hello message to peer unit 10.22.3.5, error: Unknown
 error
%ASA-1-104500: (Primary) Switching to ACTIVE - switch reason: Unable to send message to
Active unit
%ASA-5-105522: (Primary) Updating route-table wc-rt-inside
%ASA-5-105523: (Primary) Updated route-table wc-rt-inside
%ASA-5-105522: (Primary) Updating route-table wc-rt-outside
%ASA-5-105523: (Primary) Updated route-table wc-rt-outside
%ASA-5-105542: (Primary) Enabling load balancer probe responses
%ASA-5-105503: (Primary) Internal state changed from Backup to Active no peer
%ASA-5-105520: (Primary) Responding to Azure Load Balancer probes
```

Chaque journal système lié à un déploiement dans le nuage public est précédé du rôle de l'unité : (Principal) ou (Secondaire).

Messages de débogage de basculement

Pour afficher les messages de débogage, saisissez la commande **debug fover**. Consultez la référence de commande pour en savoir plus.

Remarque Étant donné que la sortie de débogage se voit attribuer une priorité élevée dans le processus du CPU, elle peut affecter considérablement les performances du système. Par conséquent, les commandes **debug fover** doivent uniquement être utilisées pour résoudre des problèmes spécifiques ou au cours de sessions de dépannage effectuées avec le TAC de Cisco.

Interruptions de basculement SNMP

Pour recevoir des alertes SNMP de journal système pour le basculement, configurez l'agent SNMP pour envoyer des alertes SNMP aux stations de gestion SNMP, définissez un hôte de journal système et compilez la MIB de journal système Cisco dans votre station de gestion SNMP.

Historique de basculement dans le nuage public

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Basculement actif/de sauvegarde sur Microsoft Azure	7.9(1)	Cette fonctionnalité a été introduite.



CHAPITRE 12

Grappe ASA pour le Secure Firewall 3100

La mise en grappe vous permet de regrouper plusieurs ASA en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités non prises en charge par la mise en grappe, à la page 432.

- À propos de la mise en grappe d'ASA, à la page 363
- Licences pour la mise en grappe d'ASA, à la page 367
- Exigences et conditions préalables à la mise en grappe ASA, à la page 369
- Lignes directrices de la mise en grappe, à la page 370
- Configurer la mise en grappe ASA, à la page 377
- Gérer les nœuds de la grappe, à la page 408
- Supervision de la grappe ASA, à la page 415
- Exemples de mise en grappe ASA, à la page 417
- Référence pour la mise en grappe, à la page 432
- Historique de la mise en grappe d'ASA pour le Secure Firewall , à la page 449

À propos de la mise en grappe d'ASA

Cette section décrit l'architecture de mise en grappe et son fonctionnement.

Intégration d'une grappe à votre réseau

La grappe se compose de plusieurs pare-feu agissant comme une seule unité. Pour agir comme une grappe, les pare-feu ont besoin de l'infrastructure suivante :

- Réseau de fond de panier isolé à grande vitesse pour la communication intra-grappe, connu sous le nom de *liaison de commande de grappe*.
- Accès de gestion à chaque pare-feu pour la configuration et la surveillance.

Exigences en matière d'infrastructure

Lorsque vous placez la grappe dans votre réseau, les routeurs en amont et en aval doivent être en mesure d'équilibrer la charge des données entrant dans la grappe et en sortant à l'aide de EtherChannels étendus. Les interfaces de plusieurs membres de la grappe sont regroupées dans un seul EtherChannel ; l'EtherChannel effectue l'équilibrage de charge entre les unités.

Membres de la grappe

Les membres de la grappe collaborent pour partager la politique de sécurité et les flux de trafic. Cette section décrit la nature de chaque rôle de membre.

Configuration du démarrage

Sur chaque appareil, vous configurez une configuration de démarrage minimale qui inclut le nom de la grappe, l'interface de la liaison de commande de grappe et les autres paramètres de la grappe. Le premier nœud sur lequel vous activez la mise en grappe devient généralement le nœud de *contrôle*. Lorsque vous activez la mise en grappe sur les nœuds suivants, ils rejoignent la grappe en tant que nœuds de *données*.

Rôles des nœuds de contrôle et de données

Un membre de la grappe est le nœud de contrôle. Si plusieurs nœuds de la grappe sont mis en ligne en même temps, le nœud de contrôle est déterminé par le paramètre de priorité dans la configuration de démarrage. La priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée. Tous les autres membres sont des nœuds de données. En règle générale, lorsque vous créez une grappe pour la première fois, le premier nœud que vous ajoutez devient le nœud de contrôle simplement parce que c'est le seul nœud de la grappe à ce moment-là.

Vous devez effectuer toute la configuration (à l'exception de la configuration de démarrage) sur le nœud de contrôle uniquement; la configuration est ensuite reproduite sur les nœuds de données. Dans le cas de ressources physiques, telles que les interfaces, la configuration du nœud de contrôle est reflétée sur tous les nœuds de données. Par exemple, si vous configurez Ethernet 1/2 comme interface interne et Ethernet 1/1 comme interface externe, ces interfaces sont également utilisées sur les nœuds de données en tant qu'interfaces interne et externe.

Certaines fonctionnalités ne sont pas évolutives en grappe, et le nœud de contrôle gère tout le trafic pour ces fonctionnalités.

Interfaces de grappe

Vous pouvez configurer des interfaces de données ou en tant qu'interfaces individuelles . Voir Interfaces de grappe, à la page 377 pour plus d'informations.

Restrictions du type d'interface

Remarque Les interfaces individuelles ne sont pas prises en charge, à l'exception d'une interface de gestion.

Liaisons de commande de grappe

Une liaison de commande de grappe est une interface matérielle dédiée que chaque unité doit allouer à la communication au sein de la grappe. Pour plus d'informations, consultez Liaison de commande de la grappe, à la page 377.

Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

Gestion de la grappe ASA

L'un des avantages de l'utilisation de la mise en grappe ASA est la facilité de gestion. Cette section décrit comment gérer la grappe.

Réseau de gestion

Nous vous recommandons de connecter toutes les unités à un seul réseau de gestion. Ce réseau est distinct de la liaison de commande de grappe.

Interface de gestion

Pour l'interface de gestion, nous vous conseillons d'utiliser l'une des interfaces de gestion dédiées. Vous pouvez configurer les interfaces de gestion en tant qu'interfaces individuelles (pour les modes routé et transparent) ou en tant qu'interface EtherChannel étendue.

Nous vous conseillons d'utiliser des interfaces individuelles pour la gestion, même si vous utilisez des EtherChannels étendus pour vos interfaces de données. Les interfaces individuelles vous permettent de vous connecter directement à chaque unité si nécessaire, tandis qu'une interface EtherChannel étendue ne permet qu'une connexion à distance à l'unité de contrôle actuelle.



Remarque vous ne pouvez pas activer le routage dynamique pour l'interface de gestion. Vous devez utiliser une route statique.

Pour une interface individuelle, l'adresse IP de la grappe principale est une adresse fixe pour la grappe qui appartient toujours à l'unité de contrôle actuelle. Pour chaque interface, vous configurez également une plage d'adresses de sorte que chaque unité, y compris l'unité de contrôle actuelle, puisse utiliser une adresse locale de la plage. L'adresse IP de la grappe principale fournit un accès de gestion cohérent à une adresse; lorsqu'une unité de contrôle change, l'adresse IP de la grappe principale est déplacée vers la nouvelle unité de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente. L'adresse IP locale est utilisée pour le routage et est également utile pour la résolution de problèmes.

Par exemple, vous pouvez gérer la grappe en vous connectant à l'adresse IP de la grappe principale, qui est toujours associée à l'unité de contrôle actuelle. Pour gérer un membre, vous pouvez vous connecter à l'adresse IP locale.

Remarque Le trafic vers la boîte doit être acheminé vers l'adresse IP de gestion du nœud; le trafic vers la boîte n'est pas transféré sur la liaison de commande de grappe vers un autre nœud.

Pour le trafic de gestion sortant tel que TFTP ou syslog, chaque unité, y compris l'unité de contrôle, utilise l'adresse IP locale pour se connecter au serveur.

Pour une interface EtherChannel étendue, vous ne pouvez configurer qu'une seule adresse IP, et cette adresse IP est toujours associée à l'unité de contrôle. Vous ne pouvez pas vous connecter directement à une unité de données à l'aide de l'interface EtherChannel; nous vous conseillons de configurer l'interface de gestion en tant qu'interface individuelle afin que vous puissiez vous connecter à chaque unité. Notez que vous pouvez utiliser un EtherChannel local au périphérique pour la gestion.

Gestion de l'unité de contrôle vs Gestion de l'unité de données

La gestion et la surveillance peuvent avoir lieu sur le nœud de contrôle. À partir du nœud de contrôle, vous pouvez vérifier les statistiques d'exécution, l'utilisation des ressources ou d'autres informations de surveillance sur tous les nœuds. Vous pouvez également transmettre une commande à tous les nœuds de la grappe et reproduire les messages de console des nœuds de données vers le nœud de contrôle.

Vous pouvez surveiller directement les nœuds de données si vous le souhaitez. Bien que cela soit également disponible à partir du nœud de contrôle, vous pouvez effectuer la gestion de fichiers sur les nœuds de données (y compris la sauvegarde de la configuration et la mise à jour des images). Les fonctions suivantes ne sont pas disponibles à partir du nœud de commande :

- Surveillance des statistiques propres à la grappe par nœud.
- Surveillance des journaux système par nœud (sauf pour les journaux système envoyés à la console lorsque la duplication de la console est activée).
- SNMP
- NetFlow

duplication de clé de chiffrement

Lorsque vous créez une clé de chiffrement sur le nœud de contrôle, la clé est répliquée sur tous les nœuds de données. Si vous avez une session SSH sur l'adresse IP de la grappe principale, vous serez déconnecté en cas de défaillance du nœud de contrôle. Le nouveau nœud de contrôle utilise la même clé pour les connexions SSH, de sorte que vous n'avez pas besoin de mettre à jour la clé d'hôte SSH mise en cache lorsque vous vous reconnectez au nouveau nœud de contrôle.

Incompatibilité d'adresse IP du certificat de connexion ASDM

Par défaut, un certificat autosigné est utilisé pour la connexion ASDM en fonction de l'adresse IP locale. Si vous vous connectez à l'adresse IP de la grappe principale à l'aide d'ASDM, un message d'avertissement concernant une adresse IP non concordante peut s'afficher, car le certificat utilise l'adresse IP locale, et non l'adresse IP de la grappe principale. Vous pouvez ignorer le message et établir la connexion ASDM. Cependant, pour éviter ce type d'avertissement, vous pouvez inscrire un certificat qui contient l'adresse IP de la grappe principale et toutes les adresses IP locales de l'ensemble d'adresses IP. Vous pouvez ensuite utiliser ce certificat pour chaque membre de la grappe. Consultez https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html pour de plus amples renseignements.

Mise en grappe inter-sites

Pour les installations inter-sites, vous pouvez profiter de la mise en grappe d'ASA tant que vous suivez les lignes directrices recommandées.

Vous pouvez configurer chaque châssis de grappe pour qu'il appartienne à un ID de site distinct.

Les ID de site fonctionnent avec des adresses MAC et des adresses IPspécifiques au site . Les paquets qui sortent de la grappe utilisent une adresse MAC et une adresse IPpropres au site, tandis que les paquets reçus par la grappe utilisent une adresse MAC et une adresse IPglobales. Cette fonctionnalité empêche les commutateurs d'apprendre la même adresse MAC globale à partir des deux sites sur deux ports différents, ce qui entraîne une oscillation MAC; au lieu de cela, ils connaissent uniquement l'adresse MAC du site. Les adresses MAC et les adresses IP spécifiques au site sont prises en charge pour le mode routé qui utilise uniquement les EtherChannels étendus.

Les ID de site sont également utilisés pour permettre la mobilité de flux à l'aide de l'inspection LISP, la localisation du directeur pour améliorer les performances et réduire la latence aller-retour pour la mise en grappe inter-sites pour les centres de données, et la redondance des sites pour les connexions où un propriétaire de secours d'un flux se trouve toujours sur un autre site que celui du propriétaire.

Consultez les sections suivantes pour en savoir plus sur la mise en grappe inter-sites :

- Dimensionnement de l'interconnexion du centre de données : Exigences et conditions préalables à la mise en grappe ASA, à la page 369
- Lignes directrices inter-sites : Lignes directrices de la mise en grappe, à la page 370
- Configurer la mobilité des flux de grappes : Configurer la mobilité des flux de grappes, à la page 405
- Activer la localisation du directeur : Configurer les paramètres de grappe ASA de base, à la page 396
- Activer la redondance de site : Configurer les paramètres de grappe ASA de base, à la page 396
- Exemples inter-sites : Exemples de mise en grappe inter-sites, à la page 427

Licences pour la mise en grappe d'ASA

Smart Software Manager standard et sur site

Chaque unité requiert la licence Essentials (activée par défaut) et la même licence de chiffrement. Nous vous conseillons d'accorder une licence à chaque unité avec le serveur de licences *avant* d'activer la mise en grappe pour éviter les problèmes de non-concordance de licences et, lors de l'utilisation de la licence de cryptage renforcé, des problèmes de chiffrement de la liaison de commande de grappe.

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence. Il n'y a pas de coût supplémentaire pour la licence de contexte sur les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, la licence Essentials est toujours activée par défaut sur toutes les unités. Vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est

également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : chaque unité demande une licence Essentials au serveur.
- Contexte : seule l'unité de contrôle demande la licence de contexte au serveur. La licence Essentials comprend 2 contextes par défaut et est présente sur tous les membres de la grappe. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité de contrôle, sont combinées jusqu'à la limite de plateformes dans une licence de grappe agrégée. Par exemple :
  - Vous avez 6 appareils Secure Firewall 3100 dans la grappe. La licence Essentials comprend 2 contextes; pour 6 unités, ces licences ajoutent jusqu'à 12 contextes. Vous configurez une licence de 20 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 32 contextes. Comme la limite de plateformes pour un châssis est de 100, la licence combinée autorise un maximum de 100 contextes; les 32 contextes sont dans la limite. Par conséquent, vous pouvez configurer jusqu'à 32 contextes sur l'unité de contrôle; chaque unité de données aura également 32 contextes par la réplication de la configuration.
  - Vous avez 3 appareils Secure Firewall 3100 dans la grappe. La licence Essentials comprend 2 contextes; pour 3 unités, ces licences ajoutent jusqu'à 6 contextes. Vous configurez une licence de 100 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 106 contextes. Comme la limite de plateformes pour une unité est de 100, la licence combinée autorise un maximum de 100 contextes; les 106 contextes sont au-dessus de la limite. Par conséquent, vous ne pouvez configurer que 100 contextes sur l'unité de contrôle; chaque unité de données aura également 100 contextes par la réplication de la configuration. Dans ce cas, vous devez uniquement configurer la licence de contexte de l'unité de contrôle pour 94 contextes.
- Cryptage renforcé (3DES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité de contrôle demande cette licence et toutes les unités peuvent l'utiliser en raison de l'agrégation des licences.

Si une nouvelle unité de contrôle est choisie, la nouvelle unité de contrôle continue d'utiliser la licence agrégée. Elle utilise également la configuration de licence mise en mémoire cache pour demander à nouveau la licence de l'unité de contrôle. Lorsque l'ancienne unité de contrôle rejoint la grappe en tant qu'unité de données, elle libère le droit de licence de l'unité de contrôle. Avant que l'unité de données ne libère la licence, la licence de l'unité de contrôle peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La licence conservée est valide pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Vous devez éviter de modifier la configuration jusqu'à ce que les demandes de licences soient complètement traitées. Si une unité quitte la grappe, la configuration de contrôle mise en mémoire cache est supprimée, tandis que les droits par unité sont conservés. En particulier, vous devrez demander à nouveau la licence de contexte sur les unités qui ne sont pas des grappes.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer la mise en grappe.

Exigences et conditions préalables à la mise en grappe ASA

Exigences du modèle

- Secure Firewall 3100 : maximum 8 nœuds

Configuration matérielle et logicielle requise pour l'ASA

Pour toutes les unités d'une grappe :

- Doivent être du même modèle et disposer de la même mémoire DRAM. Vous n'avez pas besoin d'avoir la même quantité de mémoire flash.
- Doit exécuter le logiciel identique, sauf lors d'une mise à niveau d'image. La mise à niveau rapide est prise en charge. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.
- Doivent être dans le même mode de contexte de sécurité, unique ou multiple.
- (Mode de contexte unique) Doivent utiliser le même mode de pare-feu (routé ou transparent).
- Les nouveaux membres de la grappe doivent utiliser le même paramètre de chiffrement SSL (la commande **ssl encryption**) que l'unité de contrôle pour la communication de la liaison de commande de grappe initiale avant la réplication de la configuration.

Exigences du commutateur

- Assurez-vous d'achever la configuration du commutateur avant de configurer la mise en grappe sur les ASA.
- Pour obtenir la liste des commutateurs pris en charge, consultez Compatibilité Cisco ASA.

Exigences ASA

- Fournissez à chaque unité une adresse IP unique avant de les joindre au réseau de gestion.
  - Consultez le chapitre de démarrage pour en savoir plus sur la connexion à l'ASA et la définition de l'adresse IP de gestion.
  - À l'exception de l'adresse IP utilisée par l'unité de contrôle (généralement la première unité que vous ajoutez à la grappe), ces adresses IP de gestion sont uniquement destinées à un usage temporaire.
  - Après qu'une unité de données ait rejoint la grappe, la configuration de l'interface de gestion est remplacée par celle répliquée à partir de l'unité de contrôle.

dimensionnement de l'interconnexion du centre de données pour la mise en grappe inter-sites

Vous devez réserver la bande passante sur l'interconnexion des centres de données (DCI) pour un trafic de liaison de commande de grappe équivalent au calcul suivant :



Si le nombre de membres diffère sur chaque site, utilisez le plus grand nombre pour votre calcul. La bande passante minimale pour l'interface DCI ne doit pas être inférieure à la taille de la liaison de commande de grappe pour un membre.

Par exemple :

- Pour 4 membres sur 2 sites :
  - 4 membres de la grappe au total
  - 2 membres sur chaque site
  - Liaison de commande de grappe de 5 Gbit/s par membre

  Bande passante DCI réservée = 5 Gbit/s (2/2 x 5 Gbit/s).
- Pour 6 membres sur 3 sites, la taille augmente :
  - Six membres de la grappe au total
  - 3 membres sur le site 1, 2 membres sur le site 2 et 1 membre sur le site 3
  - Liaison de commande de grappe de 10 Gbit/s par membre

  Bande passante DCI réservée = 15 Gbit/s (3/2 x 10 Gbit/s).
- Pour 2 membres sur 2 sites :
  - 2 membres de la grappe au total
  - Un membre sur chaque site
  - Liaison de commande de grappe de 10 Gbit/s par membre

  Bande passante DCI réservée = 10 Gbit/s (1/2 x 10 Gbit/s = 5 Gbit/s, mais la bande passante minimale ne doit pas être inférieure à la taille de la liaison de commande de grappe (10 Gbit/s)).

Autres exigences

Nous vous conseillons d'utiliser un serveur de terminaux pour accéder à tous les ports de console des unités membres de la grappe. Pour la configuration initiale et la gestion continue (par exemple, lorsqu'une unité tombe en panne), un serveur de terminaux est utile pour la gestion à distance.

Lignes directrices de la mise en grappe

Mode contextuel

Le mode doit correspondre sur chaque unité membre.

Mode pare-feu

Pour le mode unique, le mode de pare-feu doit correspondre sur toutes les unités.

Basculement

Le basculement n'est pas pris en charge avec la mise en grappe.

IPv6

La liaison de commande de grappe est uniquement prise en charge avec IPv4.

Commutateurs

- Assurez-vous que les commutateurs connectés correspondent aux unités de transfert maximales MTU des interfaces de données et de l'interface de liaison de commande de grappe. Vous devez configurer la MTU de l'interface de la liaison de commande de grappe pour qu'elle soit au moins 100 octets supérieure à la MTU de l'interface de données. Assurez-vous donc de configurer le commutateur de connexion de la liaison de commande de grappe correctement. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe. De plus, nous ne conseillons pas de définir la MTU de la liaison de commande de grappe entre 2 561 et 8 362. En raison de la gestion du groupe de blocs, cette taille de MTU n'est pas optimale pour le fonctionnement du système.
- Pour les systèmes Cisco IOS XR, si vous souhaitez définir une MTU autre que celle par défaut, définissez la MTU de l'interface IOS XR sur 14 octets au-dessus de la MTU du périphérique de la grappe. Sinon, les tentatives d'homologation de contiguïté OSPF peuvent échouer, sauf si l'option **mtu-ignore** est utilisée. Notez que la MTU du périphérique de grappe doit correspondre à la MTU *IPv4* d'IOS XR. Cet ajustement n'est pas nécessaire pour les commutateurs Cisco Catalyst et Cisco Nexus.
- Sur le ou les commutateurs pour les interfaces de liaison de commande de grappe, vous pouvez éventuellement activer Spanning Tree PortFast sur les ports de commutateur connectés à l'unité de la grappe pour accélérer le processus de jonction des nouvelles unités.
- Sur le commutateur, nous vous conseillons d'utiliser l'un des algorithmes d'équilibrage de charges EtherChannel suivants : **source-dest-ip** or **src-dst-mixed-ip-port** (reportez-vous à la commande **port-channel load-balance** de Cisco Nexus OS et Cisco IOS-XE). N'utilisez pas de mot clé **vlan** dans l'algorithme d'équilibrage de charge, car cela pourrait entraîner une répartition inégale du trafic vers les périphériques d'une grappe. *Ne modifiez pas* l'algorithme d'équilibrage de charge par défaut sur le périphérique de la grappe.
- Si vous modifiez l'algorithme d'équilibrage de charge de l'EtherChannel sur le commutateur, l'interface EtherChannel du commutateur arrête temporairement de transférer le trafic et le protocole Spanning Tree redémarre. Il faudra attendre un certain temps avant que le trafic ne redevienne fluide.
- Les commutateurs sur le chemin de la liaison de commande de grappe ne doivent pas vérifier la somme de contrôle L4. Le trafic redirigé sur la liaison de commande de grappe n'a pas une somme de contrôle L4 correcte. Les commutateurs qui vérifient la somme de contrôle L4 pourraient entraîner l'abandon du trafic.
- Le temps d'arrêt du groupage du canal de port ne doit pas dépasser l'intervalle Keepalive configuré.
- Sur les EtherChannels de 2e génération, l'algorithme de distribution de hachage par défaut est adaptatif. Pour éviter le trafic symétrique dans une conception VSS, modifiez l'algorithme de hachage sur le canal de port connecté au périphérique de la grappe à fixe :

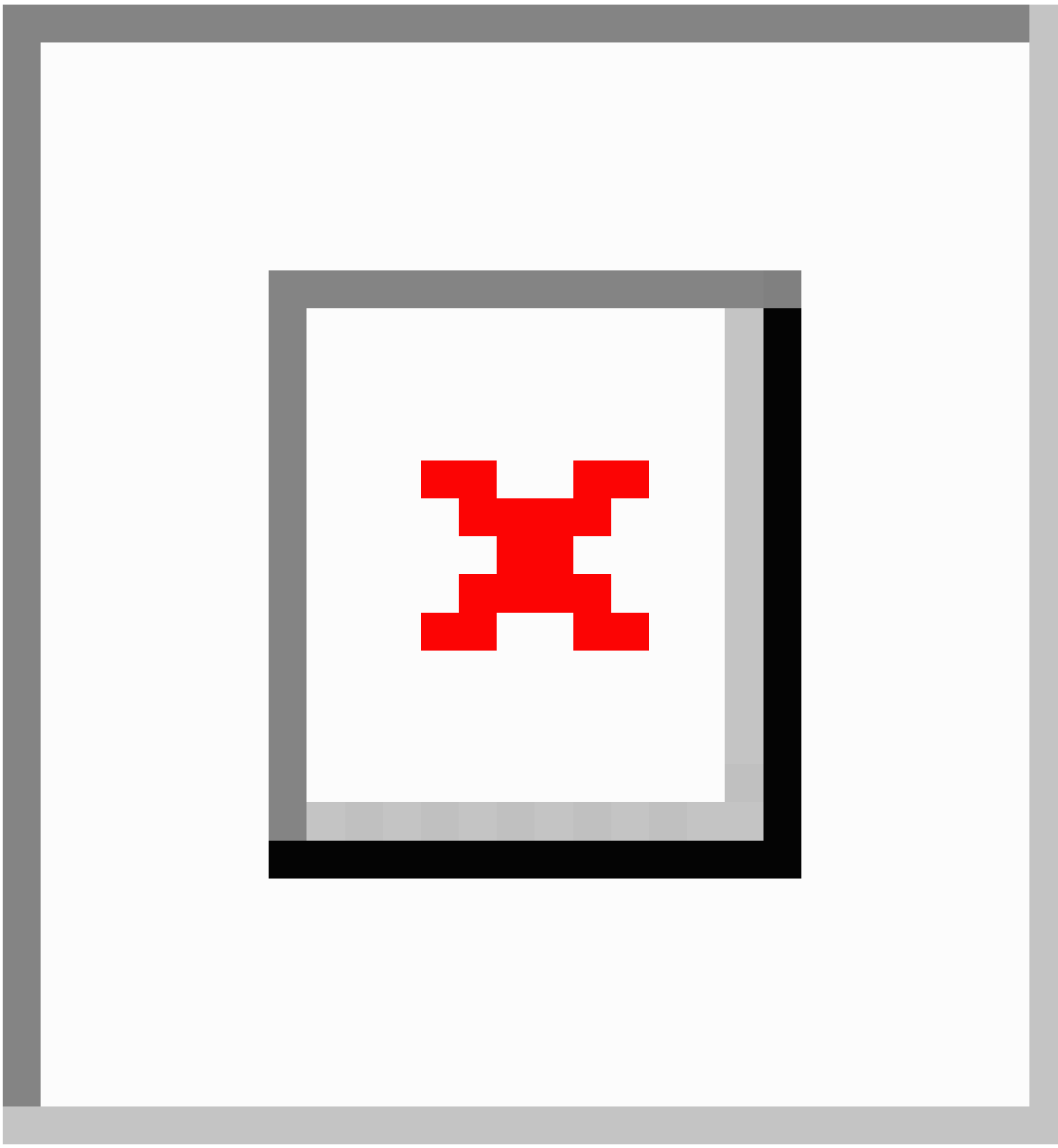
  router(config)# **port-channel** *id* **hash-distribution fixed**

Ne modifiez pas l'algorithme globalement; vous pouvez profiter de l'algorithme adaptatif pour la liaison homologue VSS.

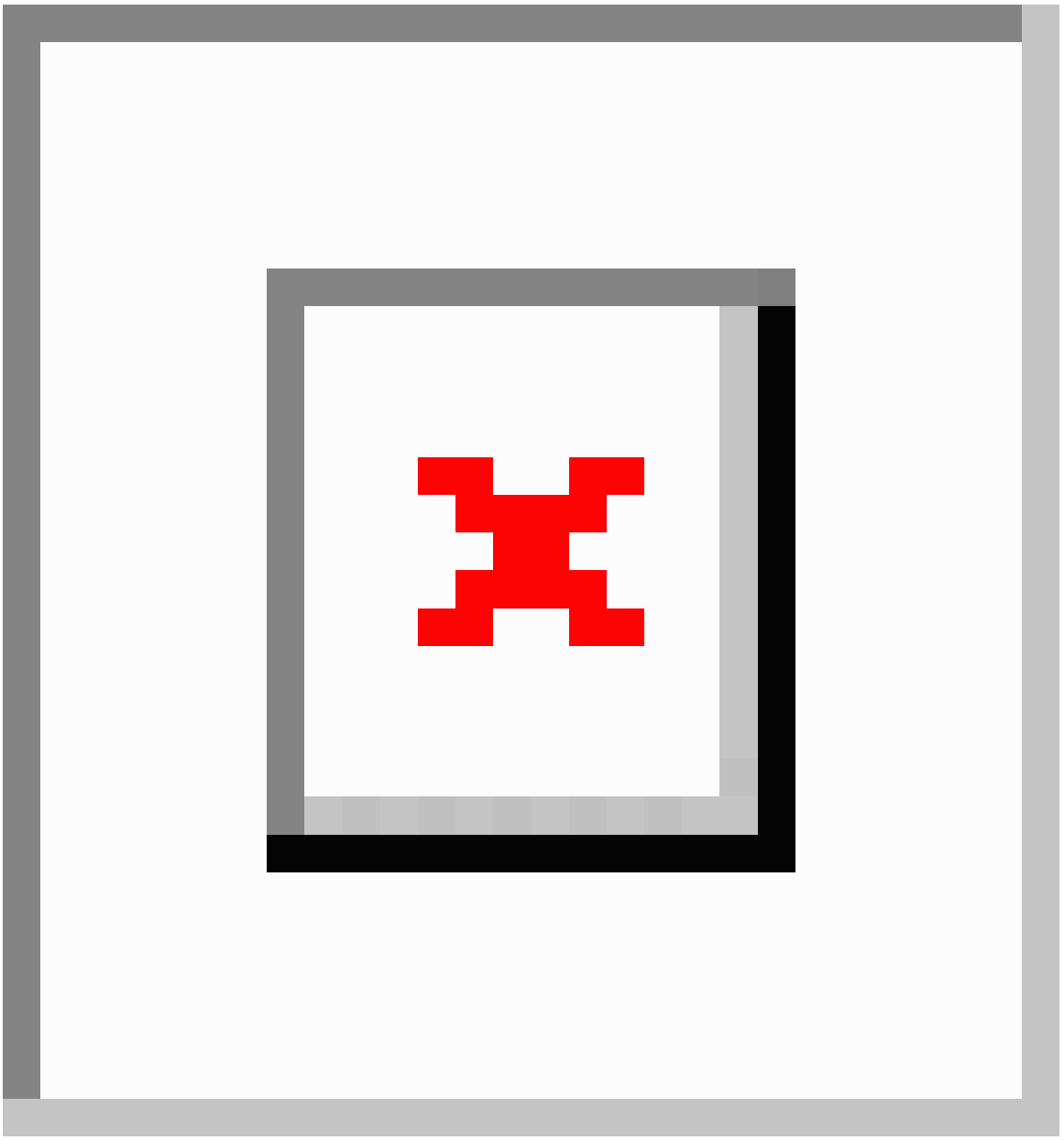
- Vous devez désactiver la fonctionnalité de convergence progressive LACP sur toutes les interfaces EtherChannel face à la grappe pour les commutateurs Cisco Nexus.

EtherChannels

- Dans les versions du logiciel Cisco IOS Catalyst 3750-X antérieures à la15.1(1)S2, l'unité de grappe ne prenait pas en charge la connexion d'un EtherChannel à une pile de commutateurs. Avec les paramètres par défaut du commutateur, si l'EtherChannel de l'unité de grappe est connecté de manière croisée et si le commutateur de l'unité de contrôle est hors tension, l'EtherChannel connecté au commutateur restant ne s'activera pas. Pour améliorer la compatibilité, définissez la commande **stack-mac persistent timer** sur une valeur suffisamment grande pour prendre en compte le temps de rechargement; par exemple, 8 minutes ou 0 pour indéfini. Vous pouvez également effectuer une mise à niveau vers une version plus stable du logiciel du commutateur, comme par exemple 15.1(1)S2.
- Configuration des EtherChannels étendus vs. locaux au périphérique : veillez à configurer le commutateur de manière appropriée pour les EtherChannels étendus par rapport aux EtherChannels locaux au périphérique.
  - EtherChannels étendus : pour les EtherChannels *étendus* des unités de grappe, qui s'étendent sur tous les membres de la grappe, les interfaces sont combinées en un seul EtherChannel sur le commutateur. Vérifiez que chaque interface se trouve dans le même groupe de canaux sur le commutateur.



- EtherChannels locaux au périphérique : pour les EtherChannels *locaux au périphérique* de grappe, y compris tous les EtherChannels configurés pour la liaison de commande de la grappe, veillez à configurer des EtherChannels isolés sur le commutateur; ne combinez pas plusieurs EtherChannels d'unités de grappe en un seul EtherChannel sur le commutateur.



Lignes directrices inter-sites

Consultez les consignes suivantes concernant la mise en grappe inter-sites :

- La latence de la liaison de commande de grappe doit être inférieure à 20 ms temps aller-retour (RTT).
- La liaison de commande de grappe doit être fiable, sans paquets dans le désordre ou abandonnés; par exemple, vous devez utiliser un lien dédié.
- Ne configurez pas le rééquilibrage de connexion; il ne faut pas que les connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

- L'ASA ne chiffre pas le trafic de données transféré sur la liaison de commande de grappe, car il s'agit d'un lien dédié, même lorsqu'il est utilisé sur une interconnexion de centre de données (DCI). Si vous utilisez la virtualisation du transport par superposition (OTV), ou étendez la liaison de commande de grappe en dehors du domaine administratif local, vous pouvez configurer le chiffrement sur vos routeurs de frontière, comme 802.1AE MacSec sur OTV.
- La mise en œuvre de la grappe ne fait pas de différence entre les membres de plusieurs sites pour les connexions entrantes; par conséquent, les rôles de connexion pour une connexion donnée peuvent s'étendre sur plusieurs sites. Il s'agit du comportement attendu. Toutefois, si vous activez la localisation de directeur, le rôle de directeur local est toujours choisi sur le même site que le propriétaire de la connexion (selon l'ID du site). En outre, le directeur local choisit un nouveau propriétaire sur le même site si le propriétaire d'origine tombe en panne (Remarque : si le trafic est dissymétrique entre les sites et qu'il y a un trafic continu en provenance du site distant après la défaillance du propriétaire d'origine, alors un nœud du site distant site peut devenir le nouveau propriétaire s'il reçoit un paquet de données pendant la fenêtre de réhébergement.).
- Pour la localisation du directeur, les types de trafic suivants ne prennent pas en charge la localisation : le trafic NAT ou PAT; trafic inspecté par SCTP; requête du propriétaire de la fragmentation.
- Dans un déploiement Nord-Sud avec des flux UDP persistants, des boucles de routage peuvent se produire si les nœuds du site propriétaire initial du flux tombent en panne, puis reviennent en ligne, ce qui entraîne une redirection du flux vers le site d'origine. Si le nouveau propriétaire, sur l'autre site, ne dispose pas d'une route vers la destination, il redirigera le flux vers Internet, créant ainsi une boucle. Dans ce cas, utilisez la commande **clear conn** sur le nouveau propriétaire pour forcer la réinitialisation du flux.
- Pour le mode transparent, si la grappe est placée entre une paire de routeurs internes et externes (AKA insertion nord-sud), vous devez vous assurer que les deux routeurs internes partagent une adresse MAC et que les deux routeurs externes partagent une adresse MAC. Lorsqu'un membre de la grappe sur le site 1 transfère une connexion à un membre du site 2, l'adresse MAC de destination est conservée. Le paquet n'atteindra le routeur du site 2 que si l'adresse MAC est la même que celle du routeur du site 1.
- Pour le mode transparent, si la grappe est placée entre les réseaux de données et le routeur de passerelle de chaque site pour le pare-feu entre les réseaux internes (AKA insertion est-ouest), chaque routeur de passerelle doit utiliser un protocole FHRP (First Hop Redundancy Protocol) comme HSRP pour fournir des destinations d'adresses IP et MAC virtuelles identiques sur chaque site. Les VLAN de données sont étendus à l'ensemble des sites à l'aide de la virtualisation du transport par superposition (OTV), ou d'un outil similaire. Vous devez créer des filtres pour empêcher le trafic destiné au routeur de la passerelle local d'être envoyé à l'autre site sur DCI. Si le routeur de la passerelle devient inaccessible sur un site, vous devez supprimer les filtres pour que le trafic puisse atteindre la passerelle de l'autre site.
- Pour le mode transparent, si la grappe est connectée à un routeur HSRP, vous devez ajouter l'adresse MAC HSRP du routeur en tant qu'entrée de tableau d'adresses MAC statiques sur ASA (voir Ajouter une adresse MAC statique pour les groupes de ponts, à la page 839). Lorsque des routeurs adjacents utilisent HSRP, le trafic destiné à l'adresse IP HSRP sera envoyé à l'adresse MAC HSRP, mais le trafic retour proviendra de l'adresse MAC de l'interface d'un routeur particulier dans la paire HSRP. Par conséquent, le tableau d'adresses MAC ASA n'est généralement mis à jour que lorsque l'entrée du tableau ARP ASA pour l'adresse IP HSRP expire et que l'ASA envoie une demande ARP et reçoit une réponse. Étant donné que les entrées du tableau ARP de l'ASA expirent après 14 400 secondes par défaut, mais que l'entrée du tableau d'adresses MAC expire après 300 secondes par défaut, une entrée d'adresse MAC statique est requise pour éviter les pertes de trafic liées à l'expiration du tableau.
- Pour le mode routé à l'aide de l'EtherChannel étendu, configurez les adresses MAC propres au site. Étendre les VLAN de données à tous les sites à l'aide d'OTV ou d'un outil similaire. Vous devez créer des filtres pour empêcher le trafic destiné à l'adresse MAC globale d'être envoyé à l'autre site par DCI.

Si la grappe devient inaccessible sur un site, vous devez supprimer les filtres pour que le trafic puisse atteindre les nœuds de la grappe de l'autre site. Le routage dynamique n'est pas pris en charge lorsqu'une grappe inter-sites sert de routeur de premier saut pour un segment étendu.

Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le pare-feu ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise, ou StackWise Virtual), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.
- Lors de l'ajout d'une unité à une grappe existante ou lors du rechargement d'une unité, il se produira une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent bloquer votre connexion; par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Si vous utilisez un serveur Windows 2003 connecté à un EtherChannel étendu, lorsque le port du serveur de journal système est en panne et que le serveur ne gère pas les messages d'erreur ICMP, un grand nombre de messages ICMP sont renvoyés à la grappe. Ces messages peuvent faire en sorte que certaines unités de la grappe connaissent un niveau élevé de CPU, ce qui peut affecter les performances. Nous vous recommandons de limiter les messages d'erreur ICMP.
- Il faut du temps pour répliquer les modifications sur toutes les unités d'une grappe. Si vous apportez une modification importante, par exemple, ajouter une règle de contrôle d'accès qui utilise des groupes d'objets (qui, lorsqu'ils sont déployés, sont divisés en plusieurs règles), le temps nécessaire pour effectuer la modification peut dépasser le délai d'expiration des unités de la grappe avec un message de réussite. Si cela se produit, vous pourriez voir le message « Échec de la réplication de la commande ». Vous pouvez ignorer le message.

Valeurs par défaut pour la mise en grappe

- Lorsque vous utilisez des EtherChannels étendus, l'ID système cLACP est généré automatiquement et la priorité du système est 1 par défaut.
- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- La fonction de jonction automatique de la grappe en cas d'échec de la liaison de commande de grappe offre des tentatives illimitées toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante effectue 3 essais toutes les 5 minutes, l'intervalle croissant étant fixé à 2.
- Le rééquilibrage de la connexion est désactivé par défaut. Si vous activez le rééquilibrage de la connexion, l'intervalle par défaut entre les échanges d'informations de chargement est de 5 secondes.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe ASA

Pour configurer la mise en grappe, effectuez les tâches suivantes.

Remarque Pour activer ou désactiver la mise en grappe, vous devez utiliser une connexion de console (pour l'interface de ligne de commande) ou une connexion ASDM.

Sauvegarder vos configurations (conseillé)

Lorsque vous activez la mise en grappe sur une unité de données, la configuration actuelle est remplacée par une configuration synchronisée à partir de l'unité active. Si vous souhaitez quitter complètement la grappe, il peut être utile d'avoir une configuration de sauvegarde avec une configuration d'interface de gestion utilisable.

Avant de commencer

Effectuez une sauvegarde sur chaque unité.

Procédure

Étape 1 Choisissez **Tools (Outils)** > **Backup Configurations (Configurations de sauvegarde)**.

Étape 2 Sauvegardez au moins la configuration en cours d'exécution. Consultez Sauvegarde et restauration de configurations ou d'autres fichiers, à la page 1203 pour connaître la procédure détaillée.

Câbler les unités et configurer les interfaces

Avant de configurer la mise en grappe, câblez le réseau de liaisons de commande de grappe, le réseau de gestion et les réseaux de données. Configurez ensuite vos interfaces.

Interfaces de grappe

Vous pouvez configurer les interfaces de données EtherChannels étendus .

Chaque unité doit également dédier au moins une interface matérielle comme liaison de commande de grappe.

Liaison de commande de la grappe

Une liaison de contrôle de grappe est une interface matérielle dédiée qui permet la communication entre les unités de grappe et prend en charge la coordination du fonctionnement de la grappe.

Chaque unité doit dédier au moins une interface matérielle comme liaison de commande de grappe. Nous vous recommandons d'utiliser un EtherChannel pour le lien de commande de grappe, si disponible.

Présentation du trafic de liaison de commande de grappe

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

Interfaces et réseau de la liaison de commande de grappe

Vous pouvez utiliser n'importe quelle interface de données pour la liaison de commande de grappe, avec les exceptions suivantes :

- Vous ne pouvez pas utiliser une sous-interface VLAN comme liaison de commande de grappe.
- Vous ne pouvez pas utiliser une interface de gestion Management *x*/*x* comme liaison de commande de grappe, seule ou en tant qu'EtherChannel.

Vous pouvez utiliser un EtherChannel.

Chaque liaison de commande de grappe possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe ASA.

Pour une grappe de deux membres, ne connectez pas directement la liaison de commande de grappe d'un nœud ASA à l'autre ASA. Si vous connectez directement les interfaces, lorsqu'une unité tombe en panne, la liaison de commande de grappe tombe en panne, et donc l'unité intègre restante. Si vous connectez la liaison de commande de grappe par l'intermédiaire d'un commutateur, cette dernière reste active pour l'unité intègre.

Dimensionnement de la liaison de commande de grappe

Le trafic de liaison de commande de grappe est principalement composé de mises à jour d'état et de paquets transférés. Le volume de trafic varie à un moment donné sur la liaison de commande de grappe. La quantité de trafic transféré dépend de l'efficacité de l'équilibrage de la charge et de l'importance du trafic pour les fonctionnalités centralisées.

Par exemple :

- La NAT entraîne un mauvais équilibrage de la charge des connexions et la nécessité de rééquilibrer tout le trafic de retour vers les bonnes unités.
- L'AAA pour l'accès réseau est une fonctionnalité centralisée, de sorte que tout le trafic est acheminé à l'unité de contrôle.
- Lorsque les membres changent, la grappe doit rééquilibrer un grand nombre de connexions, utilisant ainsi temporairement une grande quantité de bande passante de la liaison de commande de grappe.

Une liaison de commande de grappe à bande passante plus élevée aide la grappe à converger plus rapidement lorsque les membres changent et empêche les goulots d'étranglement.

Remarque Si votre grappe génère un trafic asymétrique (rééquilibreur) important, vous devez augmenter la taille du lien de commande de grappe.

Test de ping de la MTU de la liaison de commande de grappe

Utilisez les tests ping MTU de liaison de commande de grappe pour

- vérifier la compatibilité de l'unité de transfert vérifier la compatibilité de la MTU entre les nœuds de la grappe au cours du processus de jonction,
- utiliser des tests de fragmentation basés sur le ping pour confirmer que le chemin réseau prend en charge le traitement approprié des paquets, et
- permettre aux nœuds de rejoindre la grappe même si les tests échouent, tout en fournissant des messages de diagnostic pour le dépannage des incompatibilités de MTU.

Lorsqu'un nœud rejoint la grappe, le nœud de contrôle envoie un ping avec une charge utile d'une taille égale à deux fois la MTU. Ce processus teste la capacité du réseau à gérer la fragmentation des paquets, car la couche IP sous-jacente fragmentera les paquets qui dépassent la limite de MTU.

Un ping réussi confirme que le chemin réseau prend en charge une fragmentation appropriée et que la liaison de commande de grappe peut traiter de manière fiable le trafic avec la MTU configurée.

Si le ping échoue, affichez ces messages :

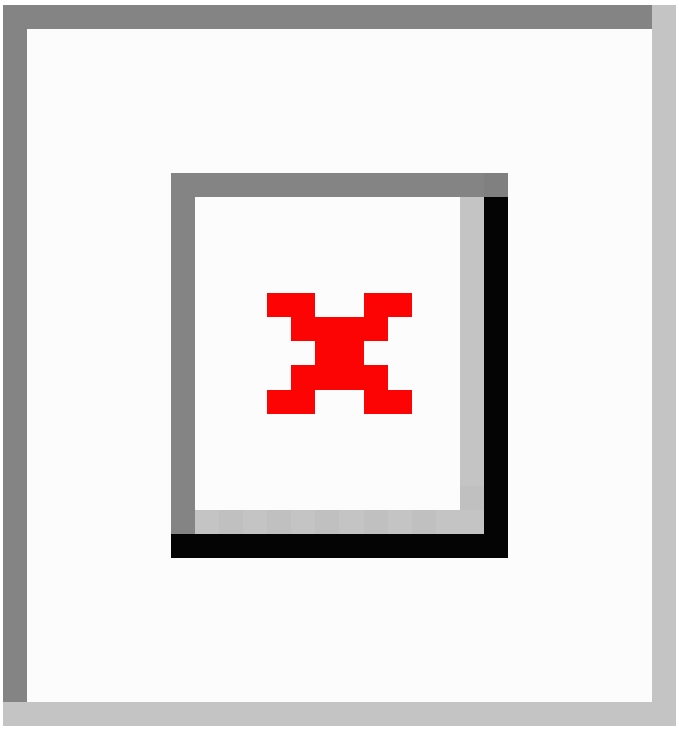
- **show cluster history**—`Événement : échec du test CCL MTU pour l'unité name`
- Console AVERTISSEMENT—`AVERTISSEMENT : L'unité name n'est pas accessible dans le test ICMP de trame étendue CCL, veuillez vérifier l'interface de grappe et la configuration MTU du commutateur.`

Même si le message ping échoue, le nœud est autorisé à rejoindre la grappe. Dans ce cas, vous devez résoudre la non-concordance de MTU dès que possible.

Redondance de la liaison de commande de la grappe

Nous vous recommandons d'utiliser un EtherChannel pour la liaison de commande de la grappe, afin de pouvoir transférer le trafic sur plusieurs liaisons de l'EtherChannel tout en assurant la redondance.

Le diagramme suivant montre comment utiliser un EtherChannel comme liaison de commande de la grappe dans un système de commutation virtuelle (VSS), un canal de port virtuel (vPC), un StackWise ou un environnement StackWise Virtual. Tous les liens de l'EtherChannel sont actifs. Lorsque le commutateur fait partie d'un système redondant, vous pouvez connecter des interfaces de pare-feu dans le même EtherChannel pour séparer les commutateurs du système redondant. Les interfaces des commutateurs sont membres de la même interface de canal de port EtherChannel, car les commutateurs distincts se comportent comme un seul commutateur. Notez qu'il s'agit d'un EtherChannel local au périphérique et non d'un EtherChannel étendu.



Fiabilité de la liaison de commande de grappe pour la mise en grappe

Pour assurer la fonctionnalité de la liaison de commande de grappe, vérifiez que le temps aller-retour (RTT) entre les unités est inférieur à 20 ms. Cette latence maximale améliore la compatibilité avec les membres de la grappe installés à différents sites géographiques. Pour vérifier votre latence, envoyez un message Ping sur la liaison de commande de grappe entre les unités.

La liaison de commande de grappe doit être fiable, sans paquets en désordre ou abandonnés; par exemple, pour un déploiement intersite, vous devez utiliser un lien dédié.

Échec de la liaison de commande de grappe

Si le protocole de liaison de commande de grappe tombe en panne pour une unité, la mise en grappe est désactivée; les interfaces de données sont fermées. Après avoir corrigé la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.

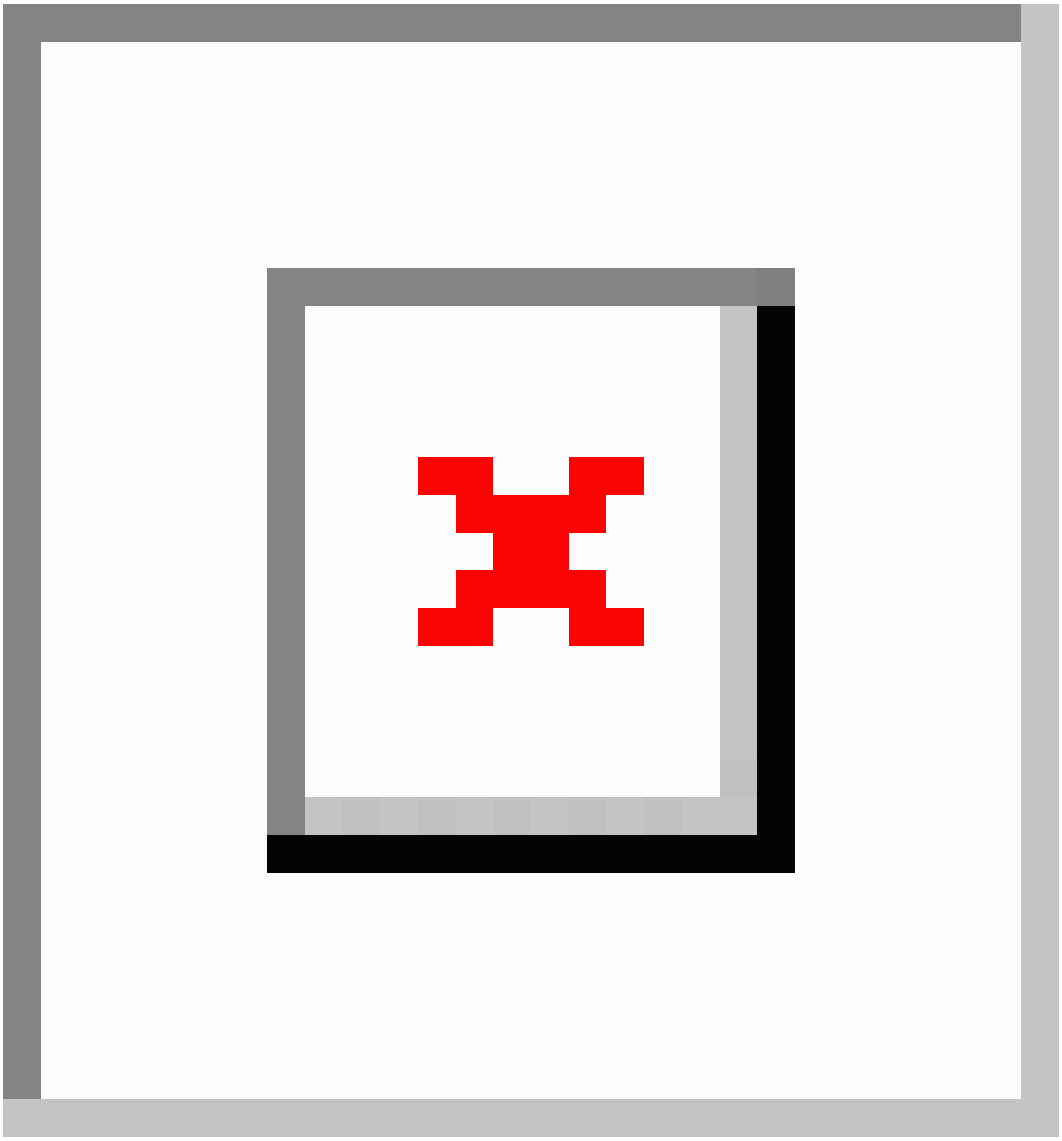
Remarque Lorsque l'ASA devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que l'unité a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que l'unité est toujours inactive dans la grappe, l'interface de gestion n'est pas accessible (car elle utilise alors l'adresse IP principale, qui est la même que l'unité de contrôle). Vous devez utiliser le port de console pour toute autre configuration.

EtherChannels étendus

Vous pouvez regrouper une ou plusieurs interfaces par châssis dans un EtherChannel qui s'étend sur tous les châssis de la grappe. L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal.

Un EtherChannel étendu peut être configuré dans les modes de pare-feu avec routage et transparent. En mode routé, l'EtherChannel est configuré comme une interface routée avec une seule adresse IP. En mode transparent, l'adresse IP est attribuée aux BVI, et non à l'interface du membre du groupe de ponts.

L'EtherChannel assure intrinsèquement l'équilibrage de la charge dans le cadre du fonctionnement de base.



Lignes directrices pour le débit maximal

Pour obtenir un débit maximal, suivez les directives suivantes :

- Utilisez un algorithme de hachage pour l'équilibrage de la charge qui est « symétrique », ce qui signifie que les paquets des deux directions auront le même hachage et seront envoyés au même ASA dans l'EtherChannel étendu. Nous vous recommandons d'utiliser l'adresse IP source et de destination (par défaut) ou les ports source et destination comme algorithme de hachage.
- Utilisez le même type de cartes de ligne lors de la connexion des ASAau commutateur afin que les algorithmes de hachage appliqués à tous les paquets soient les mêmes.

Équilibrage de charge

Le lien EtherChannel est sélectionné à l'aide d'un algorithme de hachage propriétaire, en fonction des adresses IP source ou de destination et des numéros de ports TCP et UDP.

Remarque Sur le commutateur, nous vous recommandons d'utiliser l'un des algorithmes suivants : **source-dest-IP** ou **source-dest-IP -port** (consultez la commande **d'équilibrage de la charge du canal de port** du système d'exploitation Cisco Nexus ou Cisco IOS). N'utilisez pas le mot clé **vlan** dans l'algorithme d'équilibrage de charges, car cela pourrait entraîner une répartition inégale du trafic vers les nœuds d'une grappe.

Le nombre de liaisons dans l'EtherChannel affecte l'équilibrage de la charge.

L'équilibrage de charge symétrique n'est pas toujours possible. Si vous configurez la NAT, les paquets de transfert et de retour auront des adresses IP et/ou des ports différents. Le trafic de retour sera envoyé vers une autre unité en fonction du hachage, et la grappe devra rediriger la majeure partie du trafic de retour vers la bonne unité.

Redondance EtherChannel

L'EtherChannel a une redondance intégrée. Il surveille l'état du protocole de ligne de toutes les liaisons. Si une liaison échoue, le trafic est rééquilibré entre les liaisons restantes. Si tous les liens de l'EtherChannel échouent sur une unité particulière, mais que d'autres unités sont toujours actives, cette unité est supprimée de la grappe.

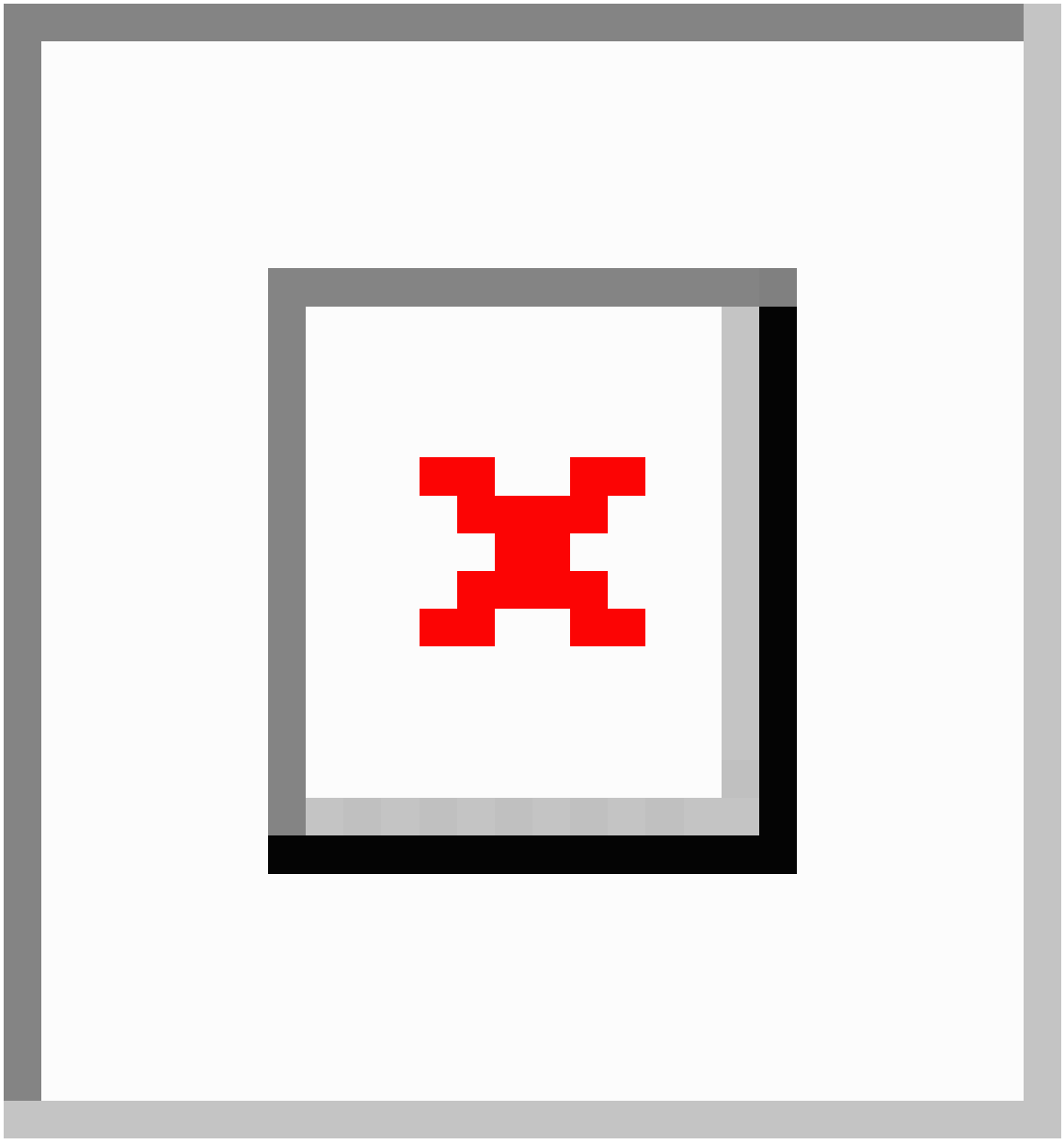
Connexion à un système de commutateurs redondants

Vous pouvez inclure plusieurs interfaces pour chaque ASA dans l'EtherChannel étendu. Plusieurs interfaces par ASA sont particulièrement utiles pour la connexion aux deux commutateurs dans un système VSS, vPC, StackWise ou StackWise Virtual.

Selon vos commutateurs, vous pouvez configurer jusqu'à 32 liens actifs dans l'EtherChannel étendu. Cette fonctionnalité nécessite que les deux commutateurs du vPC prennent en charge les canaux EtherChannels avec 16 liens actifs chacun (par exemple, le module Cisco Nexus 7000 avec le module Ethernet de 10 Gigabit de la gamme F2).

Pour les commutateurs qui prennent en charge 8 liens actifs dans l'EtherChannel, vous pouvez configurer jusqu'à 16 liens actifs dans l'EtherChannel étendu lors de la connexion à deux commutateurs dans un système redondant.

La figure suivante montre un EtherChannel de 16 liens actifs dans une grappe de 4 nœuds et une grappe de 8 nœuds.



Câbler les unités de grappe et configurer les équipements en amont et en aval

Avant de configurer la mise en grappe, câblez le réseau de liaisons de commande de grappe, le réseau de gestion et les réseaux de données.

Procédure

Étape 1 Câblez le réseau de liaisons de commande de grappe, le réseau de gestion et les réseaux de données.

Remarque Au minimum, un réseau de liaison de commande de grappe actif est requis avant de configurer les nœuds pour qu'ils se joignent à la grappe.

Étape 2 Vous devez également configurer les équipements en amont et en aval. Par exemple, si vous utilisez des EtherChannels, vous devez configurer les équipements en amont et en aval pour les EtherChannels.

Configurer le mode d'interface de grappe sur l'unité de contrôle

Avant d'activer la mise en grappe, vous devez convertir le pare-feu pour utiliser les EtherChannels étendus. Étant donné que la mise en grappe limite les types d'interfaces que vous pouvez utiliser, ce processus vous permet de vérifier votre configuration existante pour détecter les interfaces incompatibles, puis vous empêche de configurer des interfaces non prises en charge.

Remarque Si vous n'ajoutez pas d'unités de données à partir de l'unité de contrôle, vous devez définir le mode d'interface manuellement sur toutes les unités conformément à cette section, pas seulement sur l'unité de contrôle; si vous ajoutez des unités secondaires à partir de l'unité de contrôle, ASDM définit automatiquement le mode d'interface sur l'unité de données.

Avant de commencer

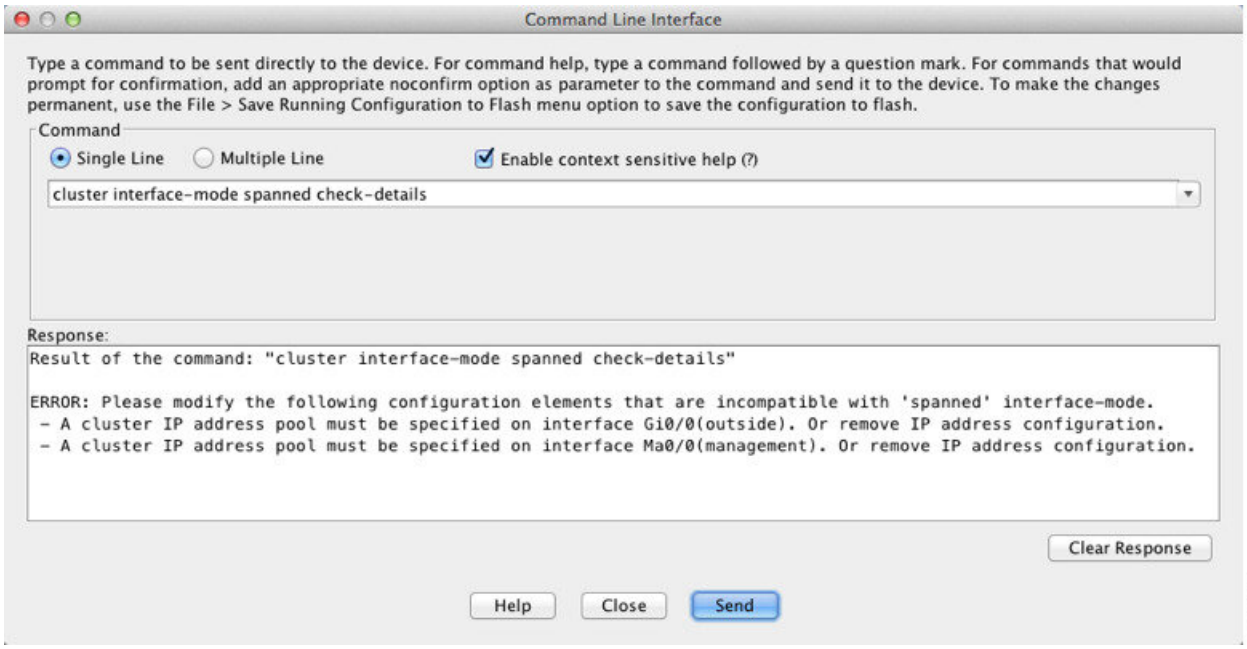
- Vous pouvez toujours configurer l'interface de gestion uniquement en tant qu'interface individuelle (conseillé). L'interface de gestion peut être une interface individuelle même en mode de pare-feu transparent.
- si vous configurez l'interface de gestion en tant qu'interface individuelle, vous ne pouvez pas activer le routage dynamique pour l'interface de gestion. Vous devez utiliser une route statique.

Procédure

Étape 1 Dans ASDM sur l'unité de contrôle, choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.Affichez toute configuration incompatible afin de pouvoir forcer le mode d'interface et corriger votre configuration ultérieurement; le mode n'est pas modifié avec cette commande :

cluster interface-mode spanned check-details

Exemple :

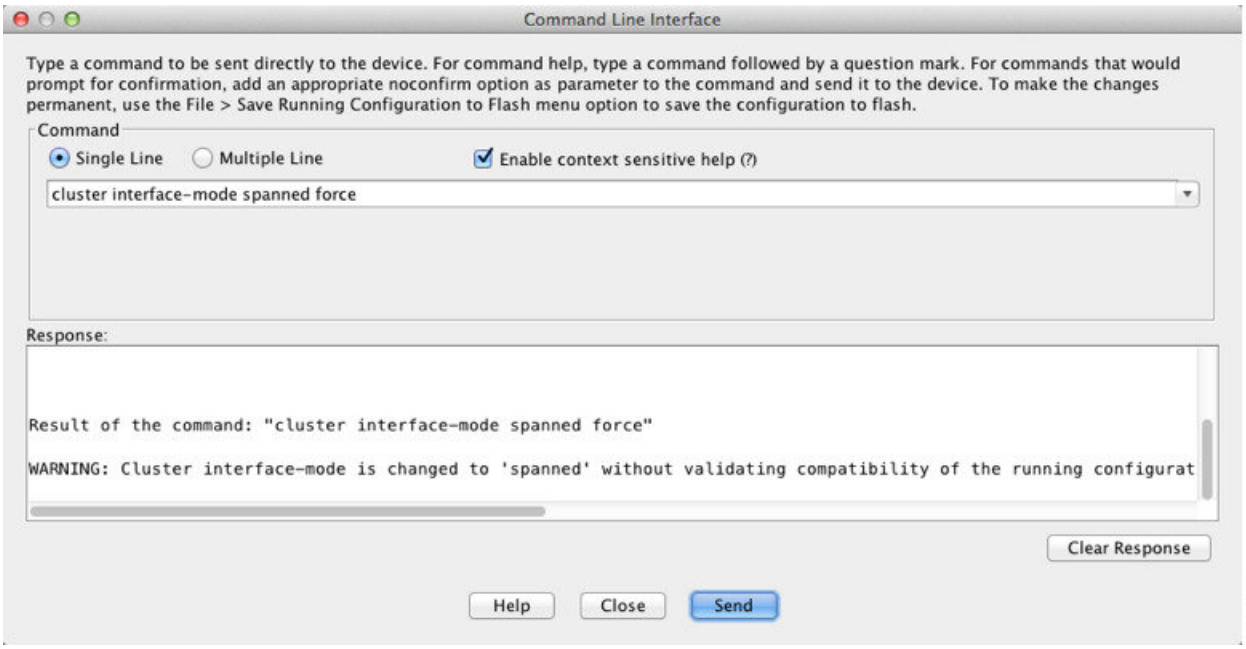


Mise en garde Après avoir défini le mode d'interface, vous pouvez continuer à vous connecter à l'interface. Cependant, si vous rechargez l'ASA avant de configurer votre interface de gestion pour respecter les exigences de la mise en grappe (par exemple, l'ajout d'un ensemble d'adresses IP de grappe), vous ne pourrez pas vous reconnecter, car la configuration d'interface incompatible avec la grappe est supprimée. Dans ce cas, vous devrez vous connecter au port de console pour corriger la configuration d'interface.

Étape 2 Définissez le mode d'interface pour la mise en grappe :

cluster interface-mode spanned force

Exemple :



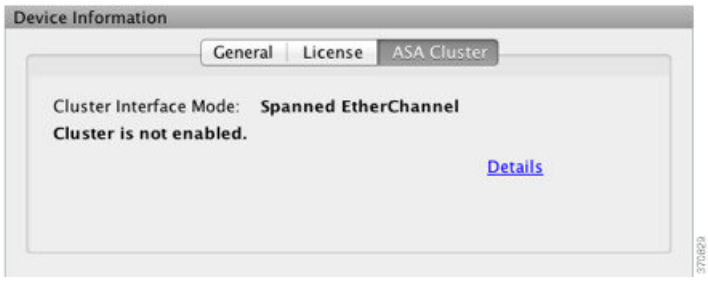
Il n'y a pas de paramètres par défaut; vous devez choisir explicitement le mode. Si vous n'avez pas défini le mode, vous ne pouvez pas activer la mise en grappe.

L'option **force** change le mode sans vérifier si votre configuration comporte des paramètres incompatibles. Vous devez résoudre manuellement tous les problèmes de configuration après avoir changé de mode. Étant donné que toute configuration d'interface ne peut être corrigée qu'après avoir défini le mode, nous vous conseillons d'utiliser l'option **force** afin de pouvoir au moins partir de la configuration existante. Vous pouvez réexécuter l'option **check-details** après avoir défini le mode pour obtenir plus de conseils.

Sans l'option **force**, en cas de configuration incompatible, vous êtes invité à effacer votre configuration et à la recharger, ce qui vous obligera à vous connecter au port de console pour reconfigurer votre accès de gestion. Si votre configuration est compatible (ce qui est rare), le mode est modifié et la configuration est conservée. Si vous ne souhaitez pas effacer votre configuration, vous pouvez quitter la commande en tapant **n**.

Pour supprimer le mode d'interface, saisissez la commande **no cluster interface-mode**.

Étape 3 Quittez ASDM et rechargez. ASDM doit être redémarré pour prendre correctement en compte le mode d'interface de la grappe. Après le rechargement, vous verrez l'onglet ASA Cluster (Grappe ASA) sur la page d'accueil :



(Recommandé; requis en mode de contexte multiple) Configurer les interfaces sur le nœud de contrôle

Vous devez modifier toute interface actuellement configurée avec une adresse IP pour qu'elle soit prête pour la grappe avant d'activer la mise en grappe. Vous devez au minimum modifier l'interface de gestion à laquelle ASDM est actuellement connecté. Pour les autres interfaces, vous pouvez les configurer avant ou après avoir activé la mise en grappe; nous vous recommandons de préconfigurer toutes vos interfaces afin que la configuration complète soit synchronisée avec les nouveaux membres de la grappe. En mode de contexte multiple, vous devez utiliser les procédures de cette section pour réparer les interfaces existantes ou pour configurer de nouvelles interfaces. Cependant, en mode unique, vous pouvez ignorer cette section et configurer les paramètres d'interface communs dans l'assistant de haute disponibilité et d'évolutivité (voir Créer ou joindre une grappe à l'aide de l'assistant de haute disponibilité, à la page 392). Notez que les paramètres d'interface avancés tels que la création des canaux EtherChannels pour les interfaces individuelles ne sont pas disponibles dans l'assistant.

Cette section décrit comment configurer les interfaces pour qu'elles soient compatibles avec la mise en grappe.

Configurer l'interface de gestion en tant qu'interface individuelle

Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre adresse IP prise dans un ensemble d'adresses IP. L'adresse IP de la grappe principale est une adresse fixe pour la grappe qui appartient toujours au nœud de contrôle.

nous conseillons de configurer l'interface de gestion en tant qu'interface individuelle. Les interfaces de gestion individuelles vous permettent de vous connecter directement à chaque unité si nécessaire, tandis qu'une interface EtherChannel étendue permet uniquement la connexion au nœud de contrôle.

Avant de commencer

- Pour le mode de contexte multiple, effectuez cette procédure dans chaque contexte. SI vous n'êtes pas déjà en mode de configuration du contexte, dans le volet Configuration > Device List (Liste des périphériques) et double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.
- (Facultatif) Configurez l'interface en tant qu'interface EtherChannel locale du périphérique et/ou configurez les sous-interfaces.
  - Dans le cas d'un EtherChannel, celui-ci est local à l'unité et n'est pas un EtherChannel étendu.
- Si vous vous connectez à distance à l'interface de gestion à l'aide d'ASDM, l'adresse IP actuelle des unités secondaires potentielles est à usage temporaire.
  - Une adresse IP sera attribuée à chaque membre dans l'ensemble d'adresses IP de la grappe défini sur l'unité principale.
  - L'ensemble d'adresses IP de la grappe ne peut pas inclure des adresses déjà utilisées sur le réseau, y compris de potentielles adresses IP secondaires.

    Par exemple :

    1. Vous configurez l'unité principale pour qu'elle utilise 10.1.1.1.
    2. Les autres unités utilisent 10.1.1.2, 10.1.1.3 et 10.1.1.4.
    3. Lorsque vous configurez l'ensemble d'adresses IP de la grappe sur l'unité principale, vous ne pouvez pas inclure les adresses .2, .3 ou .4 dans l'ensemble, car elles sont déjà utilisées.
    4. Vous devez plutôt utiliser d'autres adresses IP sur le réseau, telles que .5, .6, .7 et .8.

Remarque L'ensemble a besoin d'autant d'adresses qu'il y a de membres dans la grappe, y compris l'unité principale; l'adresse .1 d'origine est l'adresse IP principale de la grappe qui appartient à l'unité principale actuelle.

5. Après avoir rejoint la grappe, les anciennes adresses temporaires sont abandonnées et peuvent être utilisées ailleurs.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.

Étape 2 Choisissez la ligne d'interface, puis cliquez sur modifier (**Edit**). Définissez les paramètres d'interface. Consultez les consignes suivantes :

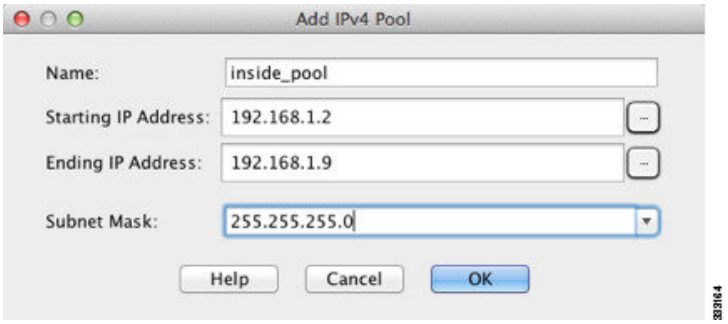
- **Dédiez cette interface à la gestion uniquement** : définit l'interface en mode gestion uniquement afin qu'elle ne transmette pas de trafic. Par défaut, les interfaces de type de gestion sont configurées en tant que gestion uniquement. En mode transparent, cette commande est toujours activée pour une interface de type de gestion.
- **Use Static IP** (Utiliser l'IP statique) : les protocoles DHCP et PPPoE ne sont pas pris en charge.

Étape 3 Pour ajouter l'ensemble d'adresses IP de la grappe IPv4, l'ensemble d'adresses MAC et les adresses MAC spécifiques au site, cliquez sur l'onglet **Advanced** (Avancé) et définissez les paramètres de la zone **ASA Cluster** (Grappe ASA).

a) Créez un ensemble d'adresses IP de grappe en cliquant sur le bouton **…** à côté du champ **IP Address Pool** (Ensemble d'adresses IP). La plage valide affichée est déterminée par l'adresse IP principale que vous avez définie dans l'onglet General (Général).

b) Cliquez sur **Add** (ajouter).

c) Configurez une plage d'adresses qui ne comprend pas l'adresse IP principale de la grappe et qui n'inclut aucune adresse actuellement utilisée sur votre réseau. Vous devez définir une plage suffisamment large pour la taille de la grappe, par exemple, 8 adresses.



d) Cliquez sur **OK** pour créer le nouvel ensemble.

e) Sélectionnez le nouvel ensemble que vous avez créé, cliquez sur **Assign** (Affecter), puis cliquez sur **OK**.

Le nom de l'ensemble apparaît dans le champ **IP Address Pool** (Ensemble d'adresses IP).

f) (Facultatif) (Facultatif) Configurez un **MAC Address Pool** (Ensemble d'adresses MAC) si vous souhaitez configurer manuellement des adresses MAC.

Étape 4 Pour configurer une adresse IPv6, cliquez sur l'onglet **IPv6**.

a) Cochez la case **Enable IPv6** (activer IPv6).

b) Dans la zone **Interface IPv6 Addresses** (Adresses IPv6 de l'interface), cliquez sur **Add** (Ajouter).

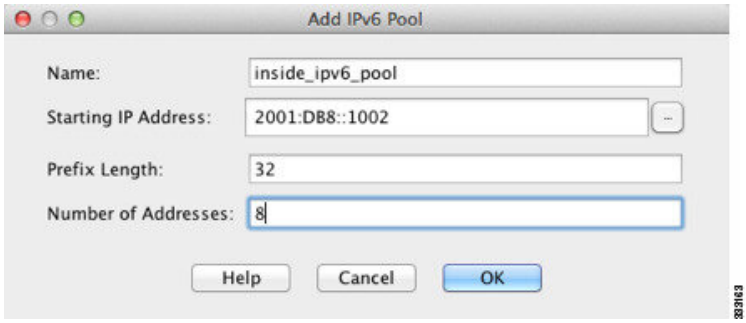
L'option **Enable address autoconfiguration** (Activer l'autoconfiguration de l'adresse) n'est pas prise en charge. La configuration manuelle de l'adresse Link-Local n'est pas non plus prise en charge.

La boîte de dialogue **Add IPv6 Address for Interface** (ajouter une adresse IPv6 pour l'interface) s'affiche.

c) Dans le champ **Address/Prefix Length** (Longueur d'adresse/préfixe), saisissez l'adresse IPv6 globale et la longueur du préfixe IPv6. Par exemple : 2001:0DB8::BA98:0:3210/48.

d) Cliquez sur le bouton **...** pour configurer l'ensemble d'adresses IP de la grappe.

e) Cliquez sur **Add** (ajouter).



f) Configurez l'adresse IP de départ (préfixe de réseau), la longueur du préfixe et le nombre d'adresses dans le groupe d'adresses.

g) Cliquez sur **OK** pour créer le nouvel ensemble.

h) Sélectionnez le nouvel ensemble que vous avez créé, cliquez sur **Assign** (Affecter), puis cliquez sur **OK**.

Le groupe apparaît dans le champ **ASA Cluster IP Pool** (Ensemble d'adresses IP de grappe ASA).

i) Cliquez sur **OK**.

Étape 5 Cliquez sur **OK** pour revenir au volet Interfaces.

Étape 6 Cliquez sur **Apply** (Appliquer).

Configurer des EtherChannel étendus

Un EtherChannel étendu couvre tous les ASA de la grappe et assure l'équilibrage de charges dans le cadre de l'opération EtherChannel.

Avant de commencer

- Vous devez être en mode d'interface EtherChannel étendu.
- Pour le mode de contexte multiple, commencez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système dans le volet Configuration > Device List (Liste des périphériques) et double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

- Pour le mode transparent, configurez le groupe de ponts. Voir Configurer la BVI (Bridge Virtual Interface), à la page 702.
- Lorsque vous utilisez des EtherChannels étendus, l'interface du canal de port ne s'affiche pas tant que la mise en grappe n'est pas complètement activée. Cette exigence empêche le trafic d'être transféré vers une unité qui n'est pas une unité active dans la grappe.

Procédure

Étape 1 Selon votre mode de contexte :

- Pour le mode unique, choisissez le volet **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces**.
- Pour le mode multiple dans l'espace d'exécution du système, choisissez le volet **Configuration > Context Management (Gestion des contextes) > Interfaces** .

Étape 2 Choisissez **Add** > **EtherChannel Interface** (Ajouter une interface EthernetChannel).

La boîte de dialogue **Add EtherChannel Interface** (Ajouter une interface EtherChannel) apparaît.

Étape 3 Activez les éléments suivants :

- **Port Channel ID** (ID du canal de port)
- **Enable Interface** (Activer l'interface) (coché par défaut)
- **Members in Group** (Membres du groupe) : dans la liste **Members in Group** (Membres du groupe), vous devez ajouter au moins une interface. Les interfaces multiples dans l'EtherChannel par unité sont utiles pour se connecter à des commutateurs dans un VSS, vPC, StackWise ou StackWise Virtual.

  Vérifiez que toutes les interfaces sont du même type et ont la même vitesse. La première interface que vous ajoutez détermine le type et la vitesse de l'EtherChannel. Toutes les interfaces non correspondantes que vous ajoutez seront mises à l'état suspendu. ASDM ne vous empêche pas d'ajouter des interfaces non correspondantes.

Les autres champs de cet écran sont décrits plus loin au cours de cette procédure.

Étape 4 Pour configurer l'adresse MAC et les paramètres facultatifs, cliquez sur l'onglet **Advanced** (Avancé).

- Dans la zone **MAC Address Cloning** (Clonage de l'adresse MAC), définissez une adresse MAC globale manuelle pour l'EtherChannel. Ne définissez pas l'adresse MAC en veille; elle est ignorée. Vous devez configurer une adresse MAC pour un EtherChannel étendu afin d'éviter d'éventuels problèmes de connectivité au réseau. Dans le cas d'une adresse MAC configurée manuellement, l'adresse MAC reste celle de l'unité de contrôle actuelle. Si vous ne configurez pas d'adresse MAC, si l'unité de contrôle change, la nouvelle unité de contrôle utilisera une nouvelle adresse MAC pour l'interface, ce qui peut provoquer une panne temporaire du réseau.

  En mode de contexte multiple, si vous partagez une interface entre les contextes, vous devez plutôt activer la génération automatique des adresses MAC pour ne pas avoir à définir l'adresse MAC manuellement. Notez que vous devez configurer manuellement l'adresse MAC à l'aide de cette commande pour les interfaces *non partagées*.

- (Mode routé) Dans la zone **ASA Cluster** (Grappe ASA), pour la mise en grappe inter-sites, définissez **Site specific MAC Addresses** (Adresses MAC spécifiques au site) pour un site en cliquant sur **Add (Ajouter)** et en spécifiant une adresse MAC et une adresse IP pour l'ID de site (1 à 8). Répétez l'opération pour un maximum de 8 sites. Les adresses IP spécifiques au site doivent se trouver sur le même sous-réseau que l'adresse IP globale. L'adresse MAC spécifique au site et l'adresse IP utilisées par une unité dépendent de l'ID de site que vous spécifiez dans la configuration de démarrage de chaque unité.

Étape 5 (Facultatif) Configurez les sous-interfaces VLAN sur cet EtherChannel. Le reste de cette procédure s'applique aux sous-interfaces.

Étape 6 (Mode de contexte multiple) Avant de terminer cette procédure, vous devez attribuer des interfaces aux contextes.

a) Cliquez sur **OK** pour accepter vos modifications.
b) Allouez les interfaces.
c) Passez au contexte que vous souhaitez configurer : dans le volet **Device List** (Liste des périphériques), double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.
d) Choisissez le volet **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces**, sélectionnez l'interface de canal de port que vous souhaitez personnaliser, puis cliquez sur **Edit**(Modifier).

   La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche.

Étape 7 Cliquez sur l'onglet **General** (Général).

Étape 8 (Mode transparent) Dans la liste déroulante **Bridge Group** (Groupe de ponts), choisissez le groupe de ponts auquel vous souhaitez affecter cette interface.

Étape 9 Dans le champ **Interface Name** (Nom d'interface), saisissez un nom renfermant au maximum 48 caractères.

Étape 10 Dans le champ **Security level** (Niveau de sécurité), saisissez un niveau compris entre 0 (le plus bas) et 100 (le plus élevé).

Étape 11 (Mode routé) Pour une adresse IPv4, cliquez sur le bouton radio **Use Static IP** (Utiliser l'adresse IP statique) et saisissez l'adresse IP et le masque. Les protocoles DHCP et PPPoE ne sont pas pris en charge. Pour les connexions point à point, vous pouvez spécifier un filtre d'adresse locale de 31 bits (255.255.255.254). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion. Pour le mode transparent, vous configurez l'adresse IP de l'interface de groupe de ponts, et non de l'interface EtherChannel.

Étape 12 (Mode routé) Pour configurer une adresse IPv6, cliquez sur l'onglet **IPv6**.

Pour le mode transparent, vous configurez l'adresse IP de l'interface de groupe de ponts, et non de l'interface EtherChannel.

a) Cochez la case **Enable IPv6** (Activer IPv6).
b) Dans la zone **Interface IPv6 Addresses** (Adresses IPv6 de l'interface), cliquez sur **Add** (Ajouter).

   La boîte de dialogue **Add IPv6 Address for Interface** (ajouter une adresse IPv6 pour l'interface) s'affiche.



Remarque L'option **Enable address autoconfiguration** (Activer l'autoconfiguration de l'adresse) n'est pas prise en charge. La configuration manuelle de l'adresse Link-Local n'est pas non plus prise en charge.

c) Dans le champ **Address/Prefix Length** (Longueur d'adresse/préfixe), saisissez l'adresse IPv6 globale et la longueur du préfixe IPv6. Par exemple, 2001:DB8::BA98:0:3210/64.

d) (Facultatif) Pour utiliser l'ID d'interface EUI-64 modifié comme adresse d'hôte, cochez la case **EUI-64**. Dans ce cas, saisissez le préfixe dans le champ **Address/Prefix Length** (Longueur d'adresse/préfixe).
e) Cliquez sur **OK**.

Étape 13 Cliquez sur **OK** pour revenir à l'écran **Interfaces**.

Étape 14 Cliquez sur **Apply** (Appliquer).

Créer ou joindre une grappe à l'aide de l'assistant de haute disponibilité

Chaque nœud de la grappe nécessite une configuration de démarrage pour rejoindre la grappe. Exécutez l'assistant de haute disponibilité et évolutivité sur un nœud (qui deviendra le nœud de contrôle) pour créer la grappe, puis ajoutez-y des nœuds de données.

Remarque L'assistant ne vous permet pas de modifier l'ID système cLACP par défaut et la priorité, qui ne peuvent être configurés que lorsque la mise en grappe est désactivée. Utilisez donc l'assistant puis désactivez la mise en grappe par la suite, ou consultez Configurer les paramètres de grappe ASA de base, à la page 396 pour configurer la grappe manuellement.

Avant de commencer

- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, dans le panneau **Configuration > Device List (Liste des périphériques)**, double-cliquez sur **System** (Système).
- Les interfaces que vous comptez utiliser pour l'interface de liaison de commande de grappe doivent être à l'état activées sur le commutateur connecté.
- Lorsque vous ajoutez un nœud à une grappe en cours d'exécution, il se peut que vous constatiez des interruptions temporaires et limitées de paquets/connexions; c'est un comportement prévu.

Procédure

Étape 1 Sélectionnez **Wizards (assistants) > High Availability and Scalability Wizard (assistant de haute disponibilité et d'évolutivité)**. Consultez les instructions relatives à l'assistant dans les étapes suivantes.

Étape 2 Dans l'écran **Interfaces**, vous ne pouvez pas créer de nouveaux canaux EtherChannels à partir de cet écran (à l'exception de la liaison de commande de grappe).

Étape 3 Dans l'écran ASA Cluster Configuration (Configuration de la grappe ASA), configurez les paramètres de démarrage, notamment :

- **Member Priority (Priorité des membres)**— Définit la priorité de ce nœud pour les élections du nœud de contrôle, entre 1 et 100, où 1 est la priorité la plus élevée.
- **Index du site** — Si vous utilisez la mise en grappe intersites, définissez l'ID de l'établissement pour ce nœud afin qu'il utilise une adresse MAC particulière à l'établissement, entre 1 et 8.

- (Facultatif) **Shared Key (Clé partagée)** : Définit une clé de chiffrement pour le trafic de contrôle sur la liaison de commande de grappe. Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères. Le secret partagé est utilisé pour générer la clé de chiffrement. Ce paramètre n'influe pas sur le trafic datapath, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair. Vous devez configurer ce paramètre si vous activez également le service de chiffrement du mot de passe.
- (Facultatif) **Enable connection rebalancing for TCP traffic across all the ASAs in the cluster (Activer le rééquilibrage de connexion pour le trafic TCP sur tous les ASA de la grappe)** : permet de rééquilibrer la connexion. Le paramètre par défaut de ce filtre est désactivé. Si cette option est activée, les ASA d'une grappe échangent périodiquement des informations de chargement et déchargent les nouvelles connexions des appareils plus chargés vers les appareils moins chargés. La fréquence, comprise entre 1 et 360 secondes, spécifie la fréquence à laquelle les informations de chargement sont échangées. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données.



Remarque Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

- (Facultatif) **Enable health monitoring of this device within the cluster** (Activer la surveillance de l'intégrité de ce périphérique au sein de la grappe) : active la fonction de vérification de l'intégrité des nœuds de la grappe. Pour déterminer l'intégrité des nœuds, les nœuds de la grappe ASA envoient des messages heartbeat keepaliveheartbeat sur la liaison de commande de grappe aux autres nœuds. Si un nœud ne reçoit pas de messages heartbeat d'un nœud homologue pendant la période d'attente, le nœud homologue est considéré comme non réactif ou mort.



Remarque Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que le changement de configuration est synchronisé avec tous les nœuds, vous pouvez réactiver le contrôle de l'intégrité.

  - **Time to Wait Before Device Considered Failed** (Temps d'attente avant que l'appareil ne soit reconnu comme défaillant) : cette valeur détermine la durée entre les messages d'état keepalive du nœud, entre .3 et 45 secondes; la valeur par défaut est de 3 secondes.
  - (Facultatif) **Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support** (Diffuser des messages keepalive sur tous les ports de liaison de commande grappe EtherChannel pour la prise en charge de VSS/vPC) : si vous configurez la liaison de commande de grappe comme EtherChannel (recommandé) et qu'il est connecté à une paire VSS ou vPC, vous devrez peut-être activer cette option. Pour certains commutateurs, lorsqu'un nœud du VSS/vPC s'arrête ou démarre, les interfaces membres d'EtherChannel connectées à ce commutateur peuvent sembler être en ligne avec l'ASA, mais elles ne font pas passer de trafic du côté du commutateur. L'ASA peut être supprimé par erreur de la grappe si vous définissez le délai d'attente

ASA selon une faible valeur (par exemple 0,8 seconde) et qu'il envoie des messages heartbeat sur l'une des interfaces EtherChannel. Lorsque vous activez cette option, l'ASA envoie des messages heartbeat sur toutes les interfaces EtherChannel dans la liaison de commande de grappe pour s'assurer qu'au moins l'un des commutateurs peut les recevoir.

- (Facultatif) **Replicate console output** (Répliquer l'extrant de la console) : permet la réplication de la console des nœuds de données vers le nœud de contrôle. Par défaut, cette fonction est désactivée. L'ASA peut imprimer certains messages directement sur la console pour certains événements critiques. Si vous activez la réplication de la console, les nœuds de données envoient les messages de la console au nœud de contrôle de sorte que vous ne devez surveiller qu'un seul port de console pour la grappe. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données.
- **Cluster Control Link** (Liaison de commande de grappe) : spécifie l'interface de liaison de commande de grappe.
  - **MTU** : spécifie le nœud de transmission maximal pour l'interface de liaison de commande de grappe qui doit être supérieur d'au moins 100 octets au MTU le plus élevé des interfaces de données, entre 1 400 et 9 198 octets, mais pas entre 2 561 et 8 362. En raison de la gestion du groupe de blocs, cette taille MTU n'est pas optimale pour le fonctionnement du système. Par défaut, la MTU est de 1500 octets.nous vous suggérons de régler le MTU au maximum. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe. Par exemple, comme la MTU maximale est de 9198 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9098, tandis que la liaison de commande de grappe peut être définie sur 9198.

Étape 4 Sur l'écran **Interfaces for Health Monitoring** (Interfaces de contrôle d'intégrité), vous pouvez exempter certaines interfaces de la surveillance en cas d'échec. Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion.



Remarque Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que le changement de configuration est synchronisé avec tous les nœuds, vous pouvez réactiver le contrôle de l'intégrité.

Étape 5 Dans l'écran **Interface Auto Rejoin settings** (Paramètres de la jonction automatique de l'interface), personnalisez les paramètres de la jonction automatique en cas de défaillance de l'interface ou de la liaison de commande de grappe. Pour chaque type, vous pouvez définir les paramètres suivants :

- **Maximum Rejoin Attempts** (Nombre maximal de tentatives de jonction) : Permet de définir le nombre de tentatives de jonction à la grappe en sélectionnant **Unlimited** (Illimité) ou une valeur comprise entre 0 et 65 535. **0** désactive la jonction automatique. La valeur par défaut est **Unlimited** (Illimité) pour l'interface de grappe et **3** pour l'interface de données.
- **Rejoin Interval** (Intervalle de jonction) : permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est **5** minutes. Le

temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.

- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente en définissant la variation d'intervalle entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente) ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l'interface de grappe et **2** pour l'interface de données.

Étape 6 Cliquez sur **Finish** (Terminer).

Étape 7 L'ASA analyse la configuration en cours à la recherche de commandes incompatibles, en vue de cerner des fonctionnalités qui ne sont pas prises en charge avec la grappe, y compris les commandes pouvant être présentes dans la configuration par défaut. Cliquez sur **OK** pour supprimer les commandes incompatibles. Si vous cliquez sur **Cancel** (annuler), la mise en grappe n'est pas activée.

Après un certain temps, pendant qu'ASDM active la mise en grappe et se reconnecte à l'ASA, l'écran d'information apparaît pour confirmer que l'ASA a été ajouté à la grappe.



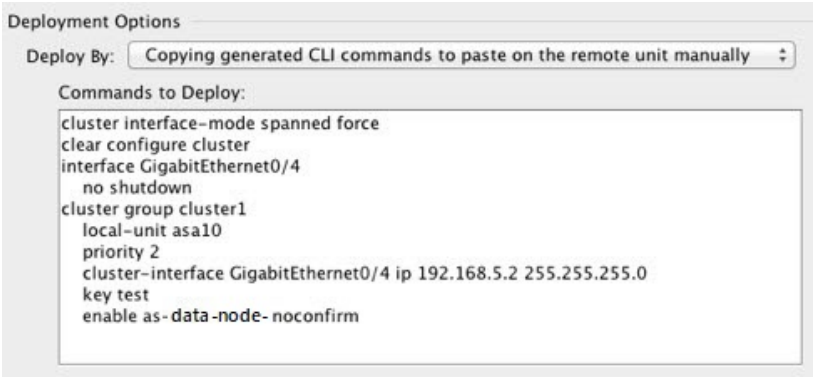
Remarque Dans certains cas, il se peut qu'une erreur se produise lors de la connexion à la grappe, une fois que le processus de l'assistant est terminé. Si ASDM a été déconnecté, ASDM ne recevra aucune erreur subséquente de l'ASA. Si la mise en grappe demeure désactivée après la reconnexion d'ASDM, vous devez vous connecter au port de console d'ASA pour déterminer la condition d'erreur exacte qui a désactivé la mise en grappe; par exemple, la liaison de commande de grappe peut être inactive.

Étape 8 Pour ajouter un nœud de données, cliquez sur **Yes (oui)**.

Si vous réexécutez l'assistant à partir du nœud de contrôle, vous pouvez ajouter des nœuds de données en choisissant l'option **Add another member to the cluster (ajouter un autre membre à la grappe)** lorsque vous lancez l'assistant pour la première fois.

Étape 9 Dans la zone des options de déploiement (**Deployment Options**), choisissez l'une des options suivantes (**Deploy By**) :

- **Envoi de commandes de l'interface de ligne de commande à l'unité distante maintenant—** Envoi de la configuration de démarrage à l'adresse IP de gestion du nœud de données (temporaire). Saisissez l'adresse IP de gestion du nœud de données, le nom d'utilisateur et le mot de passe.
- **Copie des commandes de l'interface de ligne de commande générées pour les coller manuellement sur l'unité distante**— génère les commandes afin que vous puissiez les couper et les coller sur l'interface de commande du nœud de données ou à l'aide de l'outil de l'interface de ligne de commande dans ASDM. Dans la zone des commandes à déployer, sélectionnez et copiez les commandes générées pour une utilisation ultérieure.



Personnaliser l'opération de mise en grappe

Vous pouvez personnaliser la surveillance de l'intégrité de la mise en grappe, le délai de réplication de la connexion TCP, la mobilité des flux et d'autres optimisations.

Exécutez ces procédures sur le nœud de contrôle.

Configurer les paramètres de grappe ASA de base

Vous pouvez personnaliser les paramètres de grappe sur le nœud de contrôle. Si vous n'utilisez pas l'assistant pour ajouter un nœud à la grappe, vous pouvez configurer les paramètres de grappe manuellement. Si vous avez déjà activé la mise en grappe, vous pouvez modifier certains paramètres de grappe; d'autres qui ne peuvent pas être modifiés lorsque la mise en grappe est activée sont grisés. Cette procédure inclut également les paramètres avancés qui ne sont pas inclus dans l'assistant.

Pour les paramètres qui ne peuvent être modifiés que lorsque la mise en grappe est désactivée, vous devez désactiver la mise en grappe sur tous les nœuds, puis la réactiver, ce qui nécessite un accès à l'interface de ligne de commande de la console.

Avant de commencer

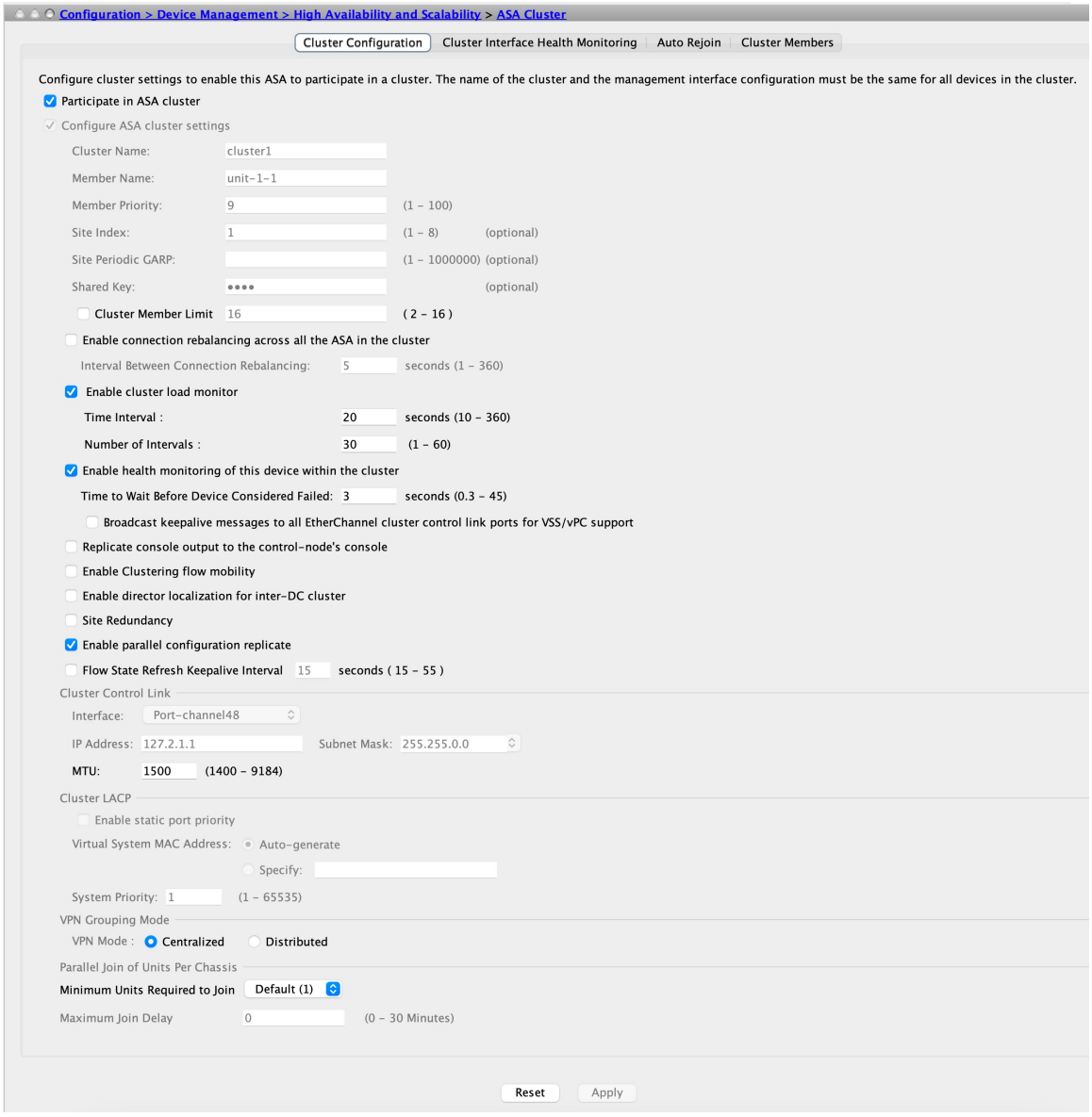
- Si vous n'avez pas utilisé l'assistant et que vous souhaitez joindre manuellement la grappe, vous devez préconfigurer les interfaces de liaison de commande de grappe sur chaque nœud avant de joindre la grappe. Pour une interface unique, vous devez l'activer; ne configurez aucun autre paramètre. Pour une interface EtherChannel, activez-la et définissez le mode EtherChannel sur Activé.
- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système sur le nœud de contrôle. Si vous n'êtes pas déjà en mode de configuration système, dans le volet **Configuration** > **Device List (Liste des périphériques)**, double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**.

Si votre périphérique est déjà dans la grappe et qu'il s'agit du nœud de contrôle, ce volet se trouve dans l'onglet **Cluster Configuration** (Configuration de la grappe).

Illustration 56 : Configuration de grappe

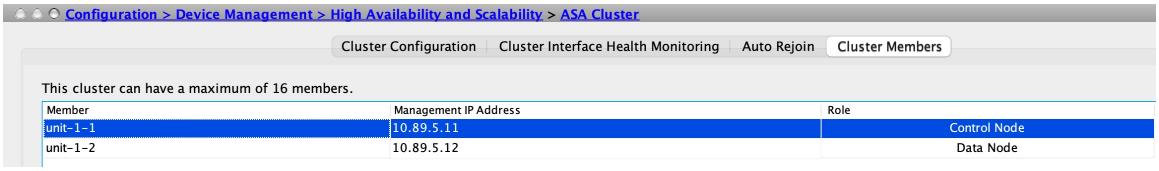


Étape 2 Si la mise en grappe a déjà été activée et que vous souhaitez configurer les paramètres grisés, désactivez la mise en grappe sur tous les nœuds.

Lorsqu'un ASA devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe, et non l'adresse IP principale.

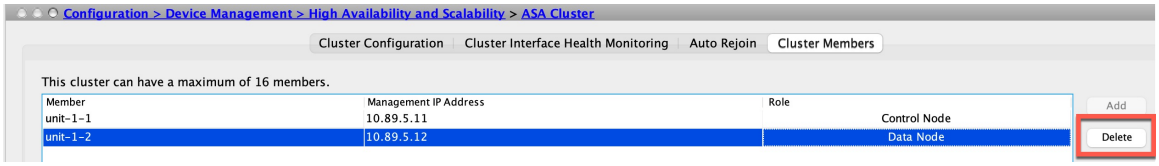
a) Vous pouvez afficher l'adresse IP locale du nœud de contrôle en cliquant sur l'onglet **Cluster Members** (Membres de la grappe). Vous devrez vous reconnecter à cette adresse après avoir désactivé la mise en grappe; veuillez donc noter l'adresse IP du nœud de contrôle.

Illustration 57 : Adresse IP de gestion du nœud de contrôle



b) Dans l'onglet **Cluster Members** (Membres de la grappe), sélectionnez chaque nœud de données, puis cliquez sur **Delete** (Supprimer).

Illustration 58 : Supprimer un nœud



La configuration de démarrage du nœud de données reste inchangée afin que vous puissiez rajouter le nœud de données ultérieurement sans perdre votre configuration.

c) Dans l'onglet **Cluster Configuration** (Configuration de la grappe), décochez la case **Participate in ASA cluster** (Participer à la grappe ASA), puis cliquez sur **Apply** (Appliquer).

Vous serez déconnecté d'ASDM.

d) Reconnectez ASDM à l'adresse IP locale du nœud de contrôle.

e) Poursuivez vos modifications conformément au reste de cette procédure. Pour configurer chaque nœud de données afin qu'il joigne la grappe après la fin de cette procédure, vous pouvez soit ajouter chaque nœud en tant que nouveau nœud, soit accéder au port de console de chaque nœud de données et réactiver la mise en grappe au niveau de l'interface de ligne de commande.

Exemple :

```
node2(config)# cluster group cluster1
node2(cfg-cluster)# enable
```

Étape 3 Cochez la case **Configure ASA cluster settings** (Configurer les paramètres de grappe ASA).

Si vous décochez la case, les paramètres sont effacés. Ne cochez pas **Participate in ASA cluster** (Participer à la grappe ASA) avant d'avoir défini tous vos paramètres.

Remarque Après avoir activé la mise en grappe, ne décochez pas la case **Configure ASA cluster settings** (Configurer les paramètres de grappe ASA) sans comprendre les conséquences. Cette action efface toute la configuration de la grappe et désactive également toutes les interfaces, y compris l'interface de gestion à laquelle ASDM est connecté. Pour rétablir la connectivité dans ce cas, vous devez accéder à l'interface de ligne de commande au niveau du port de console.

Étape 4 Configurez les paramètres de démarrage suivants :

- **Cluster Name** (Nom de la grappe) : nomme la grappe. Le nom doit être une chaîne ASCII comptant de 1 à 38 caractères. Vous ne pouvez configurer qu'une seule grappe par nœud. Tous les membres de la grappe doivent utiliser le même nom.
- **Member Name** (Nom de membre) : nomme ce membre de la grappe avec une chaîne ASCII unique de 1 à 38 caractères.
- **Member Priority** (Priorité des membres) : définit la priorité de ce nœud pour les élections du nœud de contrôle, entre 1 et 100, où 1 est la priorité la plus élevée.
- **Index du site** : si vous utilisez la mise en grappe inter-sites, définissez l'ID de site pour ce nœud afin qu'il utilise une adresse MAC propre au site, entre 1 et 8.
- (Facultatif) **Site Periodic GARP** (GARP périodique du site) : l'ASA génère des paquets ARP gratuits (GARP) pour maintenir l'infrastructure de commutation à jour : le membre ayant la priorité la plus élevée sur chaque site génère périodiquement du trafic GARP pour les adresses MAC et IP globales. Le GARP est activé par défaut lorsque vous définissez l'ID de site pour chaque nœud et l'adresse MAC et IP du site pour chaque EtherChannel étendu. Définissez l'intervalle GARP entre 1 et 1 000 000 secondes. La valeur par défaut est de 290 secondes.

  Lorsque vous utilisez des adresses MAC et IP par site, les paquets provenant de la grappe utilisent une adresse MAC et une adresse IP propres au site, tandis que les paquets reçus par la grappe utilisent une adresse MAC et une adresse IP globales. Si le trafic n'est pas généré périodiquement à partir de l'adresse MAC globale, vous pourriez rencontrer un délai d'expiration de l'adresse MAC sur vos commutateurs pour l'adresse MAC globale. Après un délai d'expiration, le trafic destiné à l'adresse MAC globale sera inondé dans l'ensemble de l'infrastructure de commutation, ce qui peut entraîner des problèmes de performance et de sécurité.
- (Facultatif) **Shared Key** (Clé partagée) : définit une clé de chiffrement pour le trafic de contrôle sur la liaison de commande de grappe. Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères. Le secret partagé est utilisé pour générer la clé de chiffrement. Ce paramètre n'influe pas sur le trafic datapath, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair. Vous devez configurer ce paramètre si vous activez également le service de chiffrement du mot de passe.
- (Facultatif) **Enable connection rebalancing for TCP traffic across all the ASAs in the cluster (Activer le rééquilibrage de connexion pour le trafic TCP sur tous les ASA de la grappe)** : permet de rééquilibrer la connexion. Le paramètre par défaut de ce filtre est désactivé. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données. Si cette option est activée, les ASA échangent périodiquement des renseignements sur les connexions par seconde et déchargent les nouvelles connexions des appareils ayant plus de connexions par seconde vers les appareils moins chargés. Les connexions existantes ne sont jamais déplacées. De plus, comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal. La fréquence, comprise entre 1 et 360 secondes, spécifie la fréquence à laquelle les informations de chargement sont échangées. La valeur par défaut est de 5 secondes.

  Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

  Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.
- **Enable cluster load monitor** (Activer le moniteur de charge de la grappe) : vous pouvez superviser la charge de trafic pour les membres de la grappe, y compris le nombre total de connexions, l'utilisation du CPU et de la mémoire, ainsi que les abandons de tampon. Si la charge est trop élevée, vous pouvez

choisir de désactiver manuellement la mise en grappe sur le nœud si les nœuds restants peuvent gérer la charge ou de régler l'équilibrage de charges sur le commutateur externe. Cette fonction est activée par défaut. Vous pouvez superviser périodiquement la charge de trafic. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur le nœud.

Définissez les paramètres suivants :

- **Time Interval** (Intervalle de temps) : définit le temps en secondes entre les messages de supervision, entre 10 et 360 secondes. La valeur par défaut est de 20 secondes.
- **Number of Intervals** (Nombre d'intervalles) : définit le nombre d'intervalles pour lesquels l'ASA conserve les données, entre 1 et 60. La valeur par défaut est 30.

Consultez **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Load-Monitoring (Supervision de la charge de la grappe)** pour afficher la charge de trafic.

- (Facultatif) **Enable health monitoring of this device within the cluster** (Activer la surveillance de l'intégrité de ce périphérique dans la grappe) : active la fonctionnalité de vérification de l'intégrité des nœuds de la grappe et détermine le temps entre les messages d'état heartbeat des nœuds, entre 0,3 et 45 secondes; la valeur par défaut est de 3 secondes. **Remarque** : lorsque vous ajoutez de nouveaux nœuds à la grappe et apportez des modifications de topologie à l'ASA ou au commutateur, vous devez désactiver temporairement cette fonctionnalité jusqu'à ce que la grappe soit terminée et désactiver la supervision d'interface pour les interfaces désactivées (**Configuration** > **Device Management [Gestion des périphériques]** > **High Availability and Scalability [Haute disponibilité et évolutivité]** > **ASA Cluster [Grappe ASA]** > **Cluster Interface Health Monitoring [Surveillance de l'intégrité de l'interface de grappe]**). Vous pouvez réactiver cette fonctionnalité une fois les modifications apportées à la grappe et à la topologie terminées. Pour déterminer l'intégrité des nœuds, les nœuds de la grappe ASA envoient des messages heartbeat keepaliveheartbeat sur la liaison de commande de grappe aux autres nœuds. Si un nœud ne reçoit pas de messages heartbeat d'un nœud homologue pendant la période d'attente, le nœud homologue est considéré comme non réactif ou mort.
  - (Facultatif) **Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support** (Diffuser des messages keepalive sur tous les ports de liaison de commande grappe EtherChannel pour la prise en charge de VSS/vPC) : si vous configurez la liaison de commande de grappe comme EtherChannel (recommandé) et qu'il est connecté à une paire VSS ou vPC, vous devrez peut-être activer cette option. Pour certains commutateurs, lorsqu'un nœud du VSS/vPC s'arrête ou démarre, les interfaces membres d'EtherChannel connectées à ce commutateur peuvent sembler être en ligne avec l'ASA, mais elles ne font pas passer de trafic du côté du commutateur. L'ASA peut être supprimé par erreur de la grappe si vous définissez le délai d'attente ASA selon une faible valeur (par exemple 0,8 seconde) et qu'il envoie des messages heartbeat sur l'une des interfaces EtherChannel. Lorsque vous activez cette option, l'ASA envoie des messages heartbeat sur toutes les interfaces EtherChannel dans la liaison de commande de grappe pour s'assurer qu'au moins l'un des commutateurs peut les recevoir.

- (Facultatif) **Debounce Time** (Délai antirebond) : configure le délai antirebond avant que l'ASA considère une interface comme défaillante et que le nœud ne soit supprimé de la grappe. Cette fonctionnalité permet une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Dans le cas d'un EtherChannel qui passe d'un état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un délai antirebond plus long peut empêcher l'interface de sembler être défaillante sur un nœud de la grappe

simplement parce qu'un autre nœud de la grappe a été plus rapide à regrouper les ports. Le délai antirebond par défaut est de 500 ms, avec une plage de 300 ms à 9 secondes.

- (Facultatif) **Replicate console output** (Répliquer l'extrant de la console) : permet la réplication de la console des nœuds de données vers le nœud de contrôle. Par défaut, cette fonction est désactivée. L'ASA peut imprimer certains messages directement sur la console pour certains événements critiques. Si vous activez la réplication de la console, les nœuds de données envoient les messages de la console au nœud de contrôle de sorte que vous ne devez surveiller qu'un seul port de console pour la grappe. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données.
- (Facultatif) **Enable Clustering Flow Mobility** (Activer la mobilité des flux de grappes). Consultez Configurer l'inspection LISP, à la page 406.
- (Facultatif) **Enable Director Localization for inter-DC cluster** (Activer la localisation de directeur pour la grappe inter-DC) : pour améliorer les performances et réduire la latence d'aller-retour dans le cas de la mise en grappe inter-sites pour les centres de données, vous pouvez activer la localisation de directeur. Les nouvelles connexions sont généralement équilibrées et appartiennent aux membres de la grappe d'un site donné. Cependant, l'ASA attribue le rôle de directeur à un membre sur *n'importe quel* site. La localisation du directeur permet des rôles de directeur supplémentaires : un directeur local sur le même site que le propriétaire et un directeur global qui peut se trouver sur n'importe quel site. Le fait de garder le propriétaire et le directeur sur le même site améliore les performances. De plus, en cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site. Le directeur global est utilisé si un membre d'une grappe reçoit des paquets pour une connexion appartenant à un autre site.
- (Facultatif) **Site Redundancy** (Redondance de site) : pour protéger les flux contre une défaillance de site, vous pouvez activer la redondance de site. Si le propriétaire de connexion de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La localisation de directeur et la redondance de site sont des fonctionnalités distinctes; vous pouvez configurer l'un ou l'autre, ou configurer les deux.
- (Facultatif) **Enable config sync acceleration** (Activer l'accélération de la synchronisation de la configuration) : lorsqu'un nœud de données a la même configuration que le nœud de contrôle, il ignorera la synchronisation de la configuration et se joindra plus rapidement. Cette fonction est activée par défaut. Cette fonctionnalité est configurée sur chaque nœud et n'est pas répliquée du nœud de contrôle au nœud de données.



Remarque Certaines commandes de configuration ne sont pas compatibles avec la jonction accélérée de grappes; si ces commandes sont présentes sur le nœud, même si la jonction accélérée de grappes est activée, la synchronisation de la configuration se produira toujours. Vous devez supprimer la configuration incompatible pour que la jonction accélérée de grappes fonctionne. Utilisez la commande **show cluster info unit-join-acceleration incompatible-config** pour afficher la configuration incompatible.

- **Enable parallel configuration replicate** (Activer la réplication de configuration parallèle) : permet au nœud de contrôle de synchroniser les modifications de configuration avec les nœuds de données en parallèle. Sinon, la synchronisation a lieu de manière séquentielle et peut prendre plus de temps.

- **Cluster Control Link** (Liaison de commande de grappe) : spécifie l'interface de liaison de commande de grappe. Aucun nom ne peut être configuré pour cette interface; les interfaces disponibles sont affichées dans la liste déroulante.
  - **Interface** : spécifie l'ID de l'interface, de préférence un EtherChannel. Les sous-interfaces et les interfaces de type de gestion ne sont pas autorisées.
  - **IP Address** (Adresse IP) : spécifie une adresse IPv4 pour l'adresse IP; IPv6 n'est pas pris en charge pour cette interface.
  - **Subnet Mask** (Filtre d'adresse locale) : spécifie le filtre d'adresse locale.
  - **MTU**— Spécifie le nœud de transmission maximal pour l'interface de liaison de commande de grappe qui doit être supérieur d'au moins 100 octets au MTU le plus élevé des interfaces de données, entre 1400 et 9198 octets. Par défaut, la MTU est de 1500 octets. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe. Nous vous suggérons de régler la MTU de liaison de commande de grappe au maximum de . Par exemple, comme la MTU maximale est de 9198 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9098, tandis que la liaison de commande de grappe peut être définie sur 9198.

- (Facultatif) **Cluster LACP** (LACP de grappe) : lorsqu'il utilise des EtherChannels étendus, l'ASA utilise cLACP pour négocier l'EtherChannel avec le commutateur voisin. Les ASA d'une grappe collaborent à la négociation du cLACP afin qu'ils apparaissent comme un seul périphérique (virtuel) pour le commutateur.
  - **Virtual System MAC Address** (Adresse MAC du système virtuel) : définit l'ID système cLACP, qui est au format d'une adresse MAC. Tous les ASA utilisent le même ID système : généré automatiquement par le nœud de contrôle (par défaut) et répliqué sur toutes les unités secondaires; ou spécifié manuellement sous le format *H.H.H*, où H est un chiffre hexadécimal de 16 bits. Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE est saisie comme suit : 000C.F142.4CDE. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données. Cependant, vous ne pouvez modifier cette valeur que si vous désactivez la mise en grappe.
  - **System Priority** (Priorité système) : définit la priorité système, entre 1 et 65535. La priorité est utilisée pour déterminer quel nœud est chargé de prendre une décision de regroupement. Par défaut, l'ASA utilise la priorité 1, qui est la priorité la plus élevée. La priorité doit être supérieure à celle du commutateur. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données. Cependant, vous ne pouvez modifier cette valeur que si vous désactivez la mise en grappe.

Étape 5 Cochez la case **Participate in ASA cluster** (Participer à la grappe ASA) pour rejoindre la grappe.

Étape 6 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de surveillance de l'intégrité de l'interface et de jonction automatique

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. Vous pouvez superviser n'importe quel ID de canal de port, ID redondant ou ID d'interface physique unique. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces

virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Interface Health Monitoring (Surveillance de l'intégrité de l'interface de grappe)**.

Étape 2 Dans la zone **Monitored Interfaces** (Interfaces surveillées), sélectionnez une interface et cliquez sur **Add** (Ajouter) pour la déplacer vers la zone **Unmonitored Interfaces** (Interfaces non surveillées).

Les messages d'état de l'interface détectent une défaillance de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Si un nœud ne reçoit pas de messages d'état d'interface dans le délai de rétention, le temps avant que l'ASA ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit un membre établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces.

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. Vous pouvez spécifier n'importe quel ID de canal de port, ID redondant ou ID d'interface physique unique. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise ou StackWise Virtual), vous devez désactiver le contrôle d'intégrité (**Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA**)) et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver le contrôle d'intégrité.

Étape 3 Cliquez sur l'onglet **Auto Rejoin** (Jonction automatique) pour personnaliser les paramètres de la jonction automatique en cas de défaillance de l'interface, du système ou de la liaison de commande de grappe. Pour chaque type, cliquez sur **Edit** (Modifier) pour définir les éléments suivants :

- **Maximum Rejoin Attempts** (Nombre maximal de tentatives de jonction) : Permet de définir le nombre de tentatives de jonction à la grappe en sélectionnant **Unlimited** (Illimité) ou une valeur comprise entre 0 et 65 535. **0** désactive la jonction automatique. La valeur par défaut est **Unlimited** (Illimité) pour l'interface de grappe et **3** pour l'interface de données et le système.
- **Rejoin Interval** (Intervalle de jonction) : permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est **5** minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente en définissant la variation d'intervalle entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente) ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la

troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l'interface de grappe et **2** pour l'interface de données et le système.

Cliquez sur **Restore Defaults** pour rétablir les paramètres par défaut.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer le délai de réplication TCP de la grappe

Activez le délai de réplication de la grappe pour les connexions TCP pour aider à éliminer le « travail inutile » lié aux flux de courte durée en retardant la création du flux directeur/de sauvegarde. Notez que si une unité tombe en panne avant la création du flux directeur/de sauvegarde, ces flux ne peuvent pas être récupérés. De même, si le trafic est rééquilibré vers une autre unité avant la création du flux, le flux ne peut pas être récupéré. Vous ne devez pas activer la réplication TCP pour le trafic sur lequel vous désactivez la répartition aléatoire TCP.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster Replication (Réplication de la grappe ASA)**.

Étape 2 Cliquez sur **Add** (Ajouter) et réglez les valeurs suivantes :

- **Replication delay** (Délai de réplication) : définissez les secondes entre 1 et 15.
- **HTTP** : définissez le délai pour tout le trafic HTTP.
- **Critères de source**
  - **Source** : définissez l'adresse IP source.
  - **Service** : (Facultatif) Définissez le port source. En général, vous définissez soit le port source, soit le port de destination, mais pas les deux.
- **Critères de destination**
  - **Source** : définissez l'adresse IP de destination.
  - **Service** : (Facultatif) Définissez le port de destination. En général, vous définissez soit le port source, soit le port de destination, mais pas les deux.

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer les fonctionnalités inter-sites

Pour la mise en grappe inter-sites, vous pouvez personnaliser votre configuration pour améliorer la redondance et la stabilité.

Configurer la mobilité des flux de grappes

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

À propos de l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux entre les sites.

À propos de LISP

La mobilité des machines virtuelles de centres de données, comme VMware VMotion, permet aux serveurs de migrer entre les centres de données tout en maintenant les connexions avec les clients. Pour prendre en charge une telle mobilité de serveur de centre de données, les routeurs doivent être en mesure de mettre à jour la route d'entrée vers le serveur lorsqu'il se déplace. L'architecture Cisco Locator/Protocole de séparation d'ID (LISP) sépare l'identité du périphérique, ou l'identifiant de terminal (EID), de son emplacement, ou localisateur de routage, dans deux espaces de numérotation différents, ce qui rend la migration du serveur transparente pour les clients. Par exemple, lorsqu'un serveur est déplacé vers un nouveau site et qu'un client envoie du trafic vers le serveur, le routeur redirige le trafic vers le nouvel emplacement.

LISP nécessite des routeurs et des serveurs dans certains rôles, tels que le routeur de tunnel de sortie (ETR) LISP, le routeur de tunnel d'entrée (ITR), les routeurs de premier saut, le résolveur de carte (MR) et le serveur de carte (MS). Lorsque le routeur du premier saut du serveur détecte que le serveur est connecté à un autre routeur, il met à jour tous les autres routeurs et les bases de données afin que l'ITR connectée au client puisse intercepter, encapsuler et envoyer le trafic vers le nouvel emplacement du serveur.

Prise en charge du LISP ASA

L'ASA n'exécute pas le LISP lui-même; il peut, cependant, inspecter le trafic LISP pour détecter les changements d'emplacement, puis utiliser ces informations pour un fonctionnement de mise en grappe transparent. Sans l'intégration du LISP, lorsqu'un serveur est déplacé vers un nouveau site, le trafic est acheminé vers un membre de la grappe ASA sur le nouveau site plutôt que vers le propriétaire d'origine du flux. Le nouvel ASA transfère le trafic vers l'ASA au niveau de l'ancien site, puis l'ancien ASA doit renvoyer le trafic vers le nouveau site pour qu'il atteigne le serveur. Ce flux de trafic est sous-optimal et est connu comme « tromboning » ou « épingle à cheveux ».

Grâce à l'intégration du LISP, les membres de la grappe ASA peuvent inspecter le trafic LISP passant entre le routeur du premier saut et l'ETR ou l'ITR, puis peuvent changer le propriétaire du flux pour qu'il se trouve sur le nouveau site.

Lignes directrices LISP

- Les membres de la grappe ASA doivent se trouver entre le routeur du premier saut et l'ITR ou l'ETR du site. La grappe ASA elle-même ne peut pas être le premier routeur de saut pour un segment étendu.
- Seuls les flux entièrement distribués sont pris en charge; les flux centralisés, les flux semi-distribués ou les flux appartenant à des nœuds individuels ne sont pas transférés vers de nouveaux propriétaires. Les flux semi-distribués comprennent des applications, telles que SIP, où tous les flux enfants appartiennent au même ASA qui possède le flux parent.
- La grappe déplace uniquement les états de flux de couche 3 et 4; certaines données d'application pourraient être perdues.
- Pour les flux de courte durée ou non essentiels pour l'entreprise, le déplacement du propriétaire peut ne pas valoir la peine. Vous pouvez contrôler les types de trafic pris en charge avec cette fonctionnalité lorsque vous configurez la politique d'inspection. Vous devez limiter la mobilité de flux au trafic essentiel.

Mise en œuvre du LISP ASA

Cette fonctionnalité comprend plusieurs configurations interdépendantes (qui sont toutes décrites dans ce chapitre) :

1. (Facultatif) Limiter les EID inspectés en fonction de l'adresse IP de l'hôte ou du serveur : le routeur de premier saut pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée, vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.
2. Inspection du trafic LISP : l'ASA inspecte le trafic LISP sur le port UDP 4342 pour détecter le message EID-notify envoyé entre le premier saut du routeur et l'ITR ou l'ETR. L'ASA gère un tableau EID qui met en corrélation l'EID et l'ID de site. Par exemple, vous devez inspecter le trafic LISP avec une adresse IP source du routeur du premier saut et une adresse de destination de l'ITR ou de l'ETR. Remarque : le trafic LISP n'a pas de directeur affecté et le trafic LISP en lui-même ne participe pas au partage de l'état de la grappe.
3. Politique de service pour activer la mobilité des flux sur le trafic spécifié : vous devez activer la mobilité des flux sur le trafic critique. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques.
4. ID de sites : l'ASA utilise l'ID de site pour chaque nœud de la grappe afin de déterminer le nouveau propriétaire.
5. Configuration au niveau de la grappe pour activer la mobilité de flux : vous devez également activer la mobilité de flux au niveau de la grappe. Ce bouton bascule marche/arrêt vous permet d'activer ou de désactiver facilement la mobilité de flux pour une classe particulière de trafic ou d'applications.

Configurer l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

Avant de commencer

- Affectez chaque unité de grappe à un ID de site en fonction de Configurer les paramètres de grappe ASA de base, à la page 396.
- Le trafic LISP n'est pas inclus dans la classe de trafic d'inspection par défaut. Vous devez donc configurer une classe distincte pour le trafic LISP dans le cadre de cette procédure.

Procédure

Étape 1 (Facultatif) Configurez une carte d'inspection LISP pour limiter les EID inspectés en fonction de l'adresse IP et pour configurer la clé partagée LISP :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **LISP**.
b) Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
c) Saisissez un nom (40 caractères maximum) et une description.
d) Pour la commande **Allowed-EID access-list**, cliquez sur **Manage** (Gérer).

Le **gestionnaire ACL** s'ouvre.

Le routeur de premier saut ou l'ITR/ETR pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée; vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.

e) Ajoutez une ACL avec au moins un ACE en fonction du guide de configuration du pare-feu.
f) Si nécessaire, saisissez la **Validation Key** (Clé de validation).

Si vous avez copié une clé chiffrée, cliquez sur le bouton radio **Encrypted** (Chiffré).

g) Cliquez sur **OK**.

Étape 2 Ajoutez une règle de politique de service pour configurer l'inspection LISP :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.
b) Cliquez sur **Add** (ajouter).
c) Dans la page **Service Policy** (Politique de service), appliquez la règle à une interface ou globalement.

Si vous avez une politique de service existante que vous souhaitez utiliser, ajoutez une règle à cette politique. Par défaut, l'ASA comprend une politique globale appelée **global_policy**. Vous pouvez également créer une politique de service par interface si vous ne souhaitez pas appliquer la politique à l'échelle mondiale. L'inspection LISP est appliquée au trafic de manière bidirectionnelle, vous n'avez donc pas besoin d'appliquer la politique de service sur les interfaces source et de destination; tout le trafic qui entre ou sort de l'interface à laquelle vous appliquez la règle est affecté si le trafic correspond à la carte dans les deux sens.

d) Sur la page **Traffic Classification Criteria** (Critères de classification du trafic), cliquez sur **Create a new traffic class** (Créer une nouvelle classe de trafic), et sous **Traffic Match Criteria** (Critères de correspondance du trafic), cochez la case **Source and Destination IP Address (uses ACL)** (Adresse IP source et de destination (utilise ACL)).
e) Cliquez sur **Next** (suivant).
f) Spécifiez le trafic que vous souhaitez inspecter. Vous devez spécifier le trafic entre le routeur de premier saut et l'ITR ou l'ETR sur le port UDP 4342. Les ACL IPv4 et IPv6 sont acceptées.
g) Cliquez sur **Next** (suivant).
h) Sur la page ou l'onglet de l'assistant **Rule Actions** (Actions de règles), sélectionnez l'onglet **Protocol Inspection** (Inspection du protocole).
i) Cochez la case **LISP**.
j) (Facultatif) Cliquez sur **Configure** (Configurer) pour choisir la carte d'inspection que vous avez créée.
k) Cliquez sur **Finish** (Terminer) pour enregistrer la règle de politique de service.

Étape 3 Ajoutez une règle de politique de service pour activer la mobilité des flux pour le trafic critique :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.
b) Cliquez sur **Add** (ajouter).
c) Sur la page **Service Policy** (Politique de service), choisissez la même politique de service que vous avez utilisée pour l'inspection LISP.
d) Sur la page **Traffic Classification Criteria** (Critères de classification du trafic), cliquez sur **Create a new traffic class** (Créer une nouvelle classe de trafic), et sous **Traffic Match Criteria** (Critères de correspondance du trafic), cochez la case **Source and Destination IP Address (uses ACL)** (Adresse IP source et de destination (utilise ACL)).
e) Cliquez sur **Next** (suivant).

f) Spécifiez le trafic opérationnel critique que vous souhaitez réaffecter au site le plus optimal lorsque les serveurs changent de site. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques. Les ACL IPv4 et IPv6 sont acceptées.

g) Cliquez sur **Next** (suivant).

h) Sur la page ou l'onglet de l'assistant **Rule Actions** (Actions de règles), sélectionnez l'onglet **Cluster** (Grappe).

i) Cochez la case **Enable Cluster flow-mobility triggered by LISP EID messages** (Activer la mobilité des flux de grappe déclenchée par les messages LISP EID).

j) Cliquez sur **Finish** (Terminer) pour enregistrer la règle de politique de service.

Étape 4 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)** > **et cochez la case Enable Clustering flow mobility** (Activer la mobilité des flux de la grappe).

Étape 5 Cliquez sur **Apply** (Appliquer).

Gérer les nœuds de la grappe

Après avoir déployé la grappe, vous pouvez modifier la configuration et gérer les nœuds de cette dernière.

Ajouter un nouveau nœud de données à partir du nœud de contrôle

Vous pouvez ajouter des nœuds de données supplémentaires à la grappe à partir du nœud de contrôle. Vous pouvez également ajouter des nœuds de données à l'aide de l'assistant de haute disponibilité et d'évolutivité. L'ajout d'un nœud de données à partir du nœud de contrôle a l'avantage de configurer la liaison de commande de grappe et de définir le mode d'interface de grappe sur chaque nœud de données que vous ajoutez.

Vous pouvez également vous connecter au nœud de données et configurer la mise en grappe directement sur ce dernier. Cependant, après avoir activé la mise en grappe, votre session ASDM sera déconnectée et vous devrez vous reconnecter.

Avant de commencer

- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, dans le panneau **Configuration > Device List (Liste des périphériques)**, double-cliquez sur **System** (Système).
- Si vous souhaitez envoyer la configuration de démarrage sur le réseau de gestion, assurez-vous que le nœud de données a une adresse IP accessible.

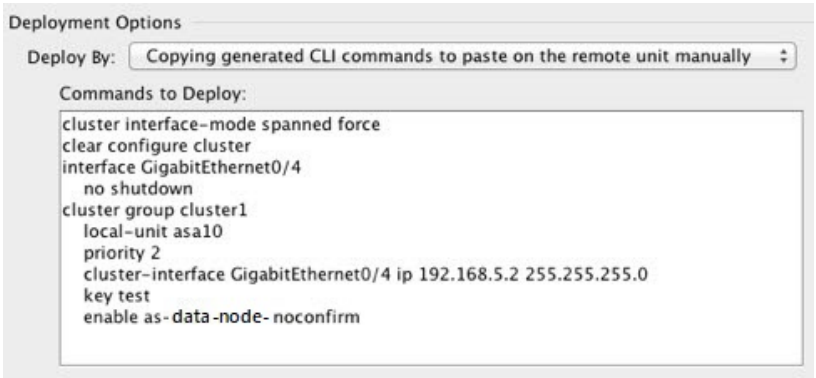
Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Members (Membres de la grappe)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Configurez selon les paramètres suivants :

- **Member Name** (Nom de membre) : nomme ce membre de la grappe avec une chaîne ASCII unique de 1 à 38 caractères.
- **Member Priority** (Priorité des membres) : définit la priorité de ce nœud pour les élections du nœud de contrôle, entre 1 et 100, où 1 est la priorité la plus élevée.
- **Cluster Control Link > IP Address** (Liaison de commande de grappe > Adresse IP) : spécifie une adresse IP unique pour ce membre pour la liaison de commande de grappe, sur le même réseau que la liaison de commande de grappe du nœud de contrôle.
- Dans la zone **Deployment Options** (Options de déploiement), choisissez l'une des options **Deploy By** (Déployer par) suivantes :
  - **Sending CLI commands to the remote unit now** (Envoi des commandes de l'interface de ligne de commande vers l'unité distante maintenant) : permet d'envoyer la configuration de démarrage à l'adresse IP de gestion (temporaire) de l'unité de données. Saisissez l'adresse IP de gestion du nœud de données, le nom d'utilisateur et le mot de passe.
  - **Copie des commandes de l'interface de ligne de commande générées pour les coller manuellement sur l'unité distante**— génère les commandes afin que vous puissiez les couper et les coller sur l'interface de commande du nœud de données ou à l'aide de l'outil de l'interface de ligne de commande dans ASDM. Dans la zone des commandes à déployer, sélectionnez et copiez les commandes générées pour une utilisation ultérieure.



Étape 4 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Devenir un nœud inactif

Pour devenir un membre inactif de la grappe, désactivez la mise en grappe sur le nœud tout en laissant intacte la configuration de mise en grappe.

Remarque Lorsqu'un ASA devient inactif (soit manuellement, soit à la suite d'un échec du contrôle d'intégrité), toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe; ou vous pouvez supprimer complètement le nœud de la grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), alors l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Avant de commencer

- Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système dans le volet Configuration > Device List (Liste des périphériques) et double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)**.

Étape 2 Décochez la case **Participer à la grappe ASA**.

Remarque Ne décochez pas la case **Configurer les paramètres de grappe ASA**. Cette action efface toute la configuration de la grappe et désactive également toutes les interfaces, y compris l'interface de gestion à laquelle ASDM est connecté. Pour rétablir la connectivité dans ce cas, vous devez accéder à l'interface de ligne de commande au niveau du port de console.

Étape 3 Cliquez sur **Apply** (Appliquer).

Désactiver un nœud de données du nœud de contrôle

Pour désactiver un nœud de données, procédez comme suit.

Remarque Lorsqu'un ASA devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Avant de commencer

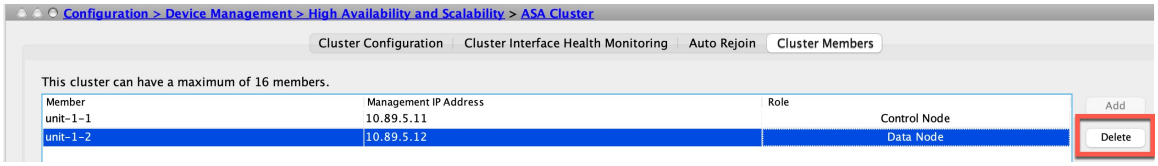
Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système dans le **volet Configuration > Device List (Liste des périphériques)** et double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Members (Membres de la grappe)**.

Étape 2 Sélectionnez le nœud de données que vous souhaitez supprimer et cliquez sur **Delete** (Supprimer).

Illustration 59 : Supprimer un nœud



La configuration de démarrage du nœud de données reste inchangée afin que vous puissiez rajouter le nœud de données ultérieurement sans perdre votre configuration.

Étape 3 Cliquez sur **Apply** (Appliquer).

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement un membre, vous devez rejoindre manuellement la grappe.

Avant de commencer

- Vous devez utiliser le port de console pour réactiver la mise en grappe. Les autres interfaces sont fermées. L'exception est que si vous avez désactivé manuellement la mise en grappe dans ASDM, vous pouvez réactiver la mise en grappe dans ASDM si vous n'avez pas enregistré la configuration et ne l'avez pas rechargée. Après le rechargement, l'interface de gestion est désactivée. L'accès à la console est donc la seule méthode pour réactiver la mise en grappe.
- Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système dans le **volet Configuration > Device List (Liste des périphériques)** et double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.
- Assurez-vous que le problème est résolu avant d'essayer de rejoindre la grappe.

Procédure

Étape 1 Si vous avez toujours l'accès à ASDM, vous pouvez réactiver la mise en grappe dans ASDM en connectant ASDM au nœud que vous souhaitez réactiver.

Vous ne pouvez pas réactiver la mise en grappe pour un nœud de données à partir du nœud de contrôle, sauf si vous l'ajoutez en tant que nouveau membre.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**.
b) Cochez la case **Participate in ASA cluster** (Participer à la grappe ASA).
c) Cliquez sur **Apply** (Appliquer).

Étape 2 Si vous ne pouvez pas utiliser ASDM : Sur la console, passez en mode de configuration de grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 3 Activez la mise en grappe.

enable

Quitter la grappe

Si vous souhaitez quitter complètement la grappe, vous devez supprimer toute la configuration de démarrage de la grappe. Étant donné que la configuration actuelle sur chaque nœud est la même (synchronisée à partir de l'unité active), quitter la grappe implique également de restaurer une configuration antérieure à la grappe à partir d'une sauvegarde ou d'effacer votre configuration et de recommencer pour éviter les conflits d'adresses IP.

Avant de commencer

Vous devez utiliser le port de console; lorsque vous supprimez la configuration de la grappe, toutes les interfaces sont fermées, y compris l'interface de gestion et la liaison de commande de grappe.

Procédure

Étape 1 Pour un nœud de données, désactivez la mise en grappe :

cluster group *cluster_name* **no enable**

Exemple :

```
ciscoasa(config)# cluster group cluster1
```

```
ciscoasa(cfg-cluster)# no enable
```

Vous ne pouvez pas modifier la configuration lorsque la mise en grappe est activée sur un nœud de données.

Étape 2 Effacez la configuration de la grappe :

clear configure cluster

L'ASA désactive toutes les interfaces, y compris l'interface de gestion et la liaison de commande de grappe.

Étape 3 Désactivez le mode d'interface de la grappe :

no cluster interface-mode

Le mode n'est pas stocké dans la configuration et doit être réinitialisé manuellement.

Étape 4 Si vous avez une configuration de sauvegarde, copiez-la dans la configuration en cours d'exécution :

copy *backup_cfg* **running-config**

Exemple :

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

Étape 5 Enregistrez la configuration pour le démarrage :

write memory

Étape 6 Si vous n'avez pas de configuration de sauvegarde, reconfigurez l'accès de gestion. Par exemple, assurez-vous de modifier les adresses IP de l'interface et de restaurer le bon nom d'hôte.

Modifier le nœud de contrôle



Mise en garde La méthode recommandée pour changer le nœud de contrôle est de désactiver la mise en grappe sur celui-ci en attendant un nouveau choix de contrôle, puis de réactiver la mise en grappe. Si vous devez spécifier le nœud exact que vous souhaitez voir devenir le nœud de contrôle, utilisez la procédure décrite dans cette section. Notez toutefois que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle à l'aide de cette procédure, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Pour modifier le nœud de contrôle, procédez comme suit.

Avant de commencer

Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système dans le volet Configuration > Device List (Liste des périphériques) et double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Summary (Résumé de la grappe)**.

Étape 2 Dans la liste déroulante, choisissez un nœud de données pour devenir le contrôle et cliquez sur le bouton pour en faire le nœud de contrôle.

Étape 3 Vous êtes invité à confirmer le changement de nœud de contrôle. Cliquez sur **Oui**.

Étape 4 Quittez ASDM et reconnectez-vous en utilisant l'adresse IP de la grappe principale.

Exécuter une commande à l'échelle de la grappe

Pour envoyer une commande à tous les nœuds de la grappe ou à un nœud en particulier, procédez comme suit. L'envoi d'une commande **show** à tous les nœuds collecte toutes les sorties et les affiche sur la console du nœud actuel. D'autres commandes, telles que **capture** et **copy**, peuvent également profiter d'une exécution à l'échelle de la grappe.

Avant de commencer

Effectuez cette procédure au niveau de l'outil d'interface de ligne de commande : choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

Procédure

Envoyez une commande à tous les nœuds ou, si vous spécifiez le nom du nœud, à un nœud en particulier :

cluster exec [**unit** *node_name*] *command*

Exemple :

```
ciscoasa# cluster exec show xlate
```

Pour afficher les noms de nœud, saisissez **cluster exec unit ?** (unité d'exécution de grappe?) (pour voir tous les noms à l'exception du nœud actuel), ou saisissez la commande **show cluster info**.

Exemples

Pour copier simultanément le même fichier de capture de tous les nœuds de la grappe vers un serveur TFTP, saisissez la commande suivante sur le nœud de contrôle :

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Plusieurs fichiers PCAP, un pour chaque nœud, sont copiés sur le serveur TFTP. Le nom du fichier de capture de destination est automatiquement associé au nom du nœud, par exemple capture1_asa1.pcap, capture1_asa2.pcap, etc. Dans cet exemple, asa1 et asa2 sont des noms de nœuds de grappe.

L'exemple de sortie suivant pour la commande **cluster exec show port-channel summary** affiche les renseignements de l'EtherChannel pour chaque nœud de la grappe :

```
ciscoasa# cluster exec show port-channel summary
control node(LOCAL):**********************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 slave:***********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

Supervision de la grappe ASA

Vous pouvez superviser et dépanner l'état de la grappe et les connexions.

Supervision de l'état de la grappe

Consultez les écrans suivantes pour superviser l'état de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Cluster Summary (Résumé de la grappe)**

  Ce volet affiche des renseignements sur la grappe concernant le nœud auquel vous êtes connecté, ainsi que les autres nœuds de la grappe. Vous pouvez également modifier le nœud principal à partir de ce volet.

- **Tableau de bord de la grappe**

  Sur la page d'accueil du nœud principal, vous pouvez superviser la grappe à l'aide des tableaux de bord de grappe et de pare-feu de grappe.

Capture des paquets à l'échelle de la grappe

Consultez l'écran suivante pour capturer des paquets dans une grappe :

Wizards (Assistants) > Packet Capture Wizard (Assistant de capture de paquets)

Pour prendre en charge le dépannage à l'échelle de la grappe, vous pouvez activer la capture du trafic spécifique à la grappe sur le nœud de contrôle, qui est ensuite automatiquement activée sur tous les nœuds de données de la grappe.

Supervision des ressources de la grappe

Consultez les écrans suivants pour surveiller les ressources de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > System Resources Graphs (Graphiques de ressources système) > CPU (Processeur)**

  Ce volet vous permet de créer des graphiques ou des tableaux montrant l'utilisation du processeur sur les nœuds de la grappe.

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > System Resources Graphs (Graphiques de ressources système) > Memory (Mémoire)**. Ce volet vous permet de créer des graphiques ou des tableaux montrant la mémoire libre et la mémoire utilisée sur les nœuds de la grappe.

Supervision du trafic de la grappe

Consultez les commandes suivants pour superviser le trafic de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Trafic Graphs (Graphiques du trafic) > Connections (Connexions)**.

  Ce volet vous permet de créer des graphiques ou des tableaux montrant les connexions entre les membres de la grappe.

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Trafic Graphs (Graphiques du trafic) > Throughput (Débit)**.

  Ce volet vous permet de créer des graphiques ou des tableaux montrant le débit du trafic entre les membres de la grappe.

- **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Load-Monitoring (Supervision de la charge de la grappe)**

  Cette section comprend les volets **Load Monitor-Information** (Renseignements sur le moniteur de charge) et **Load-Monitor Details** (Détails du moniteur de charge). **Load Monitor-Information** (Renseignements sur le moniteur de charge) affiche la charge de trafic pour les membres de la grappe pour le dernier intervalle ainsi que la moyenne du nombre total d'intervalles configurés (30 par défaut). Utilisez le volet **Load-Monitor Details** (Détails du moniteur de charge) pour afficher la valeur de chaque mesure à chaque intervalle.

Supervision de la liaison de commande de grappe

Consultez l'écran suivant pour superviser l'état de la grappe :

Monitoring (Supervision) > Properties (Propriétés) > System Resources Graphs (Graphiques des ressources du système) > Cluster Control Link (Liaison de commande de grappe).

Ce volet vous permet de créer des graphiques ou des tableaux indiquant l'utilisation de la capacité de réception et de transmission de la liaison de commande de grappe.

Supervision du routage de la grappe

Consultez l'écran suivant pour le routage de la grappe :

- **Monitoring (Supervision)** > **Routing (Routage)** > **LISP-EID Table (Tableau LISP-EID)**

  Affiche le tableau EID de l'ASA qui indique les EID et les ID de site.

Configuration de la journalisation pour la mise en grappe

Consultez l'écran suivante pour configurer la journalisation pour la mise en grappe :

Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Setup (Configuration du journal système)

Chaque nœud de la grappe génère des messages de journal système de manière indépendante. Vous pouvez pour générer des messages de journal système avec des ID de périphérique identiques ou différents afin de faire apparaître les messages comme provenant de nœuds identiques ou différents dans la grappe.

Exemples de mise en grappe ASA

Ces exemples incluent toutes les configurations ASA liées aux grappes pour les déploiements typiques.

Exemple de configuration ASA et du commutateur

Les exemples de configuration suivants connectent les interfaces suivantes entre l'ASA et le commutateur :

Interface ASA	Interface du commutateur
Ethernet 1/2	GigabitEthernet 1/0/15
Ethernet 1/3	GigabitEthernet 1/0/16
Ethernet 1/4	GigabitEthernet 1/0/17
Ethernet 1/5	GigabitEthernet 1/0/18

Configuration ASA

Mode d'interface sur chaque unité

```
cluster interface-mode spanned force
```

Configuration de démarrage de l'unité de contrôle ASA1

```
interface Ethernet1/6
 channel-group 1 mode on
 no shutdown
!
interface Ethernet1/7
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
```

```
 description Clustering Interface
!
cluster group Moya
 local-unit A
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
 priority 10
 key emphyri0
 enable noconfirm
```

Configuration de démarrage de l'unité de données ASA2

```
interface Ethernet1/6
 channel-group 1 mode on
 no shutdown
!
interface Ethernet1/7
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
 key emphyri0
 enable as-data-node
```

Configuration de l'interface de l'unité de contrôle

```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface Ethernet1/2
 channel-group 10 mode active
 no shutdown
!
interface Ethernet1/3
 channel-group 10 mode active
 no shutdown
!
interface Ethernet1/4
 channel-group 11 mode active
 no shutdown
!
interface Ethernet1/5
 channel-group 11 mode active
 no shutdown
!
interface Management1/1
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
 no shutdown
!
interface Port-channel10
 mac-address aaaa.bbbb.cccc
 nameif inside
```

```
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 mac-address aaaa.dddd.cccc
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

Configuration du commutateur Cisco IOS

```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

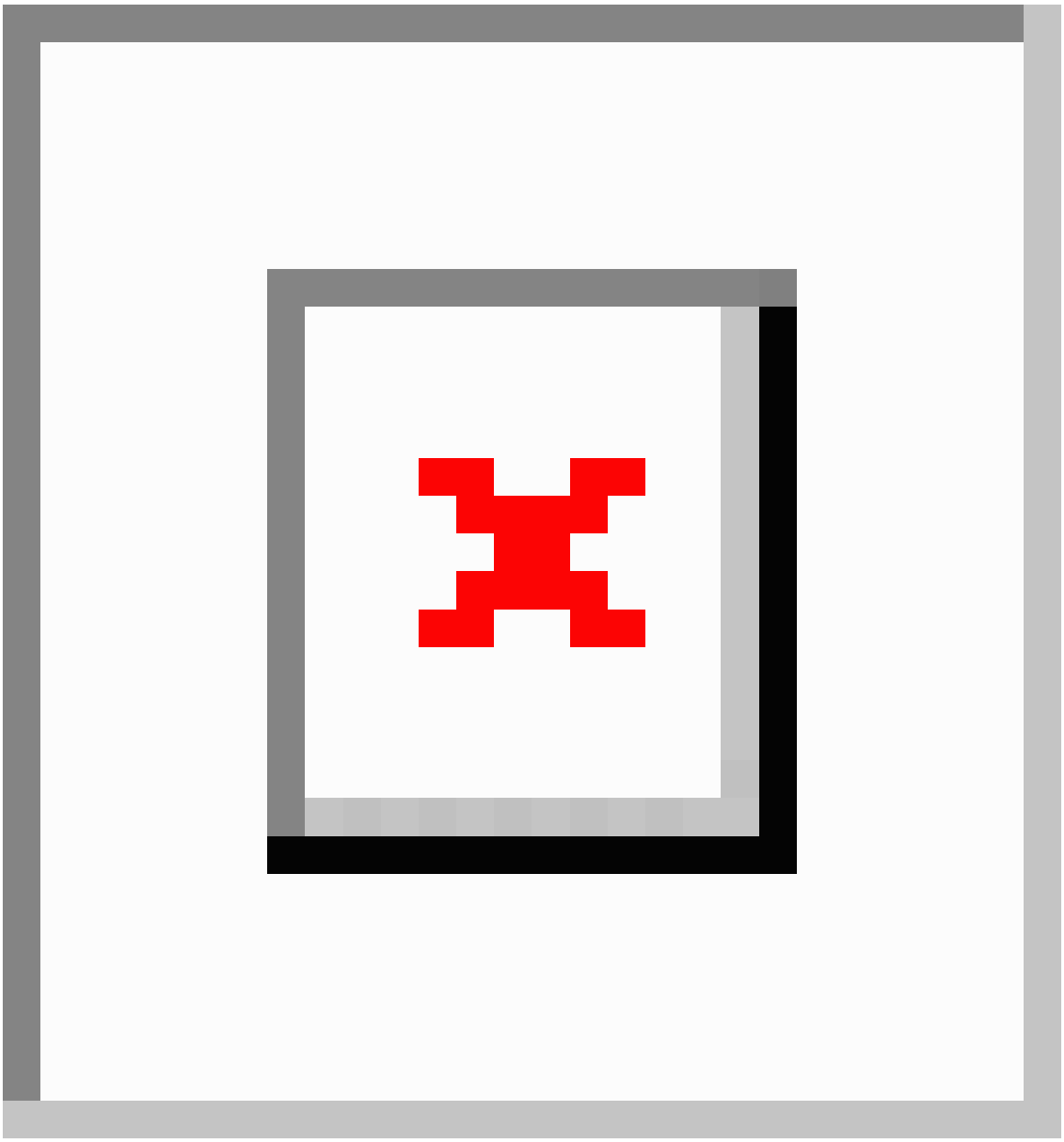
interface Port-channel10
 switchport access vlan 201
 switchport mode access

interface Port-channel11
 switchport access vlan 401
 switchport mode access
```

Pare-feu sur une seule interface

Le trafic de données de différents domaines de sécurité est associé à différents VLAN. Par exemple, VLAN 10 pour le réseau interne et VLAN 20 pour le réseau externe. Chaque ASA dispose d'un seul port physique connecté au commutateur ou routeur externe. Le regroupement de liaisons est activé de sorte que tous les paquets sur la liaison physique soient encapsulés dans une norme 802.1q. L'ASA sert de pare-feu entre le VLAN 10 et le VLAN 20.

Lorsque vous utilisez des EtherChannels étendus, toutes les liaisons de données sont regroupées dans un seul EtherChannel du côté du commutateur. Si l'ASA n'est plus disponible, le commutateur rééquilibre le trafic entre les unités restantes.



Mode d'interface sur chaque unité

```
cluster interface-mode spanned force
```

Configuration de démarrage de l'unité de contrôle de l'unité 1

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
```

```
local-unit asa1
cluster-interface ethernet1/8 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

Configuration de démarrage de l'unité de données de l'unité 2

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa2
cluster-interface ethernet1/8 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-data-node
```

Configuration de démarrage de l'unité de données de l'unité 3

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa3
cluster-interface ethernet1/8 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-data-node
```

Configuration de l'interface de l'unité de contrôle

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
no shutdown

interface ethernet1/1
channel-group 1 mode active
no shutdown

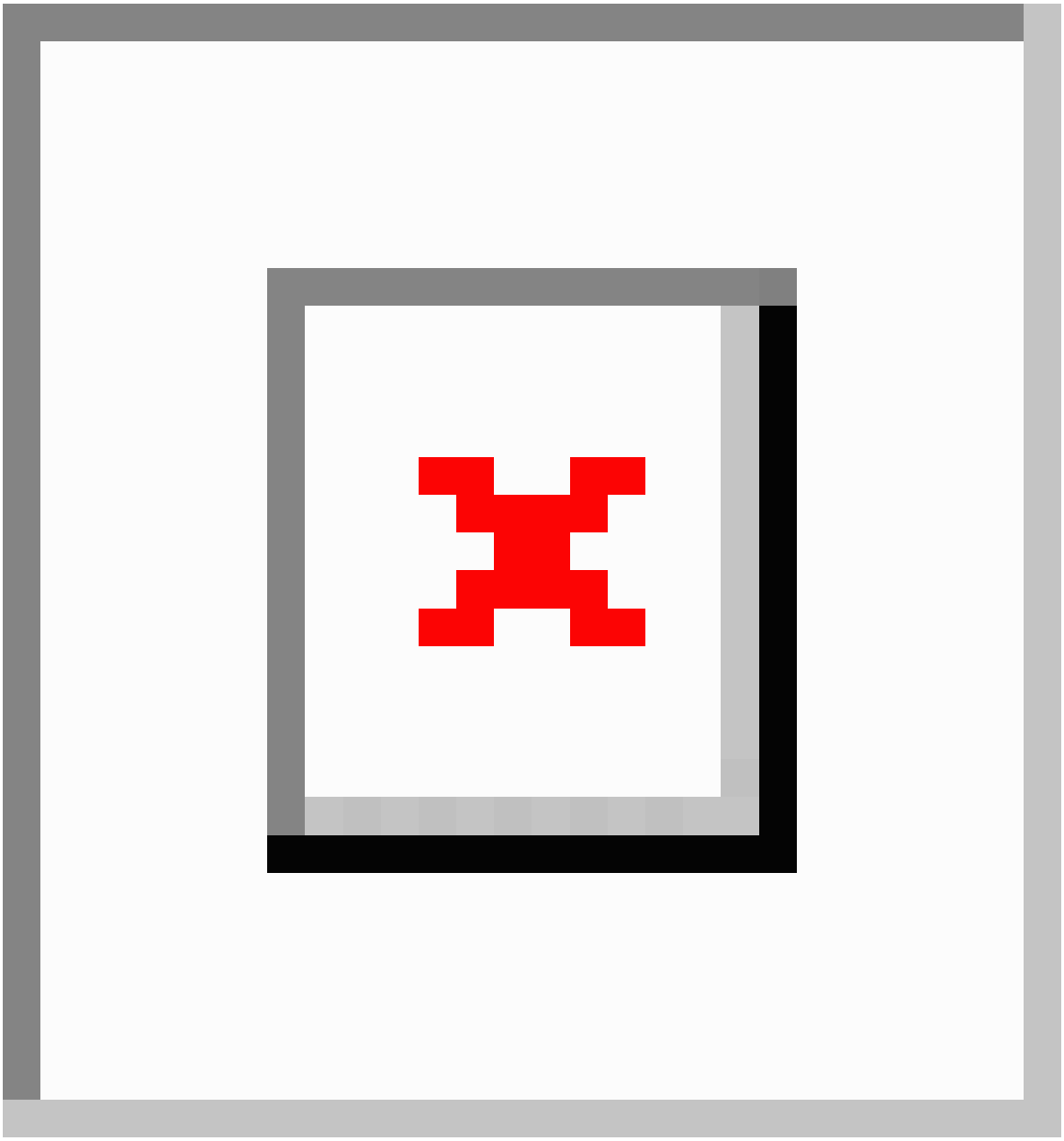
interface port-channel 1

interface port-channel 1.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE
```

```
interface port-channel 1.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

Séparation du trafic

Vous pourriez souhaiter une séparation physique du trafic entre le réseau interne et le réseau externe.



Comme le montre le diagramme ci-dessus, il y a un EtherChannel étendu sur le côté gauche qui se connecte au commutateur interne et l'autre sur le côté droit au commutateur externe. Vous pouvez également créer des sous-interfaces VLAN sur chaque EtherChannel, au besoin.

Mode d'interface sur chaque unité

```
cluster interface-mode spanned force
```

Configuration de démarrage de l'unité de contrôle de l'unité 1

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa1
 cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
 priority 1
 key chuntheunavoidable
 enable noconfirm
```

Configuration de démarrage de l'unité de données de l'unité 2

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa2
 cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
 priority 2
 key chuntheunavoidable
 enable as-data-node
```

Configuration de démarrage de l'unité de données de l'unité 3

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
```

```
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa3
 cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
 priority 3
 key chuntheunavoidable
 enable as-data-node
```

Configuration de l'interface de l'unité de contrôle

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
 nameif management
 ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
 ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
 security-level 100
 management-only
 no shutdown

interface ethernet 1/8
 channel-group 2 mode active
 no shutdown

interface port-channel 2
 nameif inside
 ip address 10.10.10.5 255.255.255.0
 ipv6 address 2001:DB8:1::5/64
 mac-address 000C.F142.4CDE

interface ethernet 2/1
 channel-group 3 mode active
 no shutdown

interface port-channel 3
 nameif outside
 ip address 209.165.201.1 255.255.255.224
 ipv6 address 2001:DB8:2::8/64
 mac-address 000C.F142.5CDE
```

Configuration OTV pour la mise en grappe inter-sites en mode routé

La réussite de la mise en grappe inter-sites pour le mode routé avec les EtherChannels étendus dépend de la configuration et de la supervision appropriées de l'OTV. L'OTV joue un rôle majeur en transférant les paquets sur l'interface DCI. L'OTV transfère les paquets de monodiffusion sur l'interface DCI uniquement lorsqu'il apprend l'adresse MAC dans sa table de transfert. Si l'adresse MAC n'est pas apprise dans la table de transfert OTV, il abandonnera les paquets de monodiffusion.

Exemple de configuration OTV

```
//Sample OTV config:
```

```
//3151 – Inside VLAN, 3152 – Outside VLAN, 202 – CCL VLAN
//aaaa.1111.1234 – ASA inside interface global vMAC
//0050.56A8.3D22 – Server MAC

feature ospf
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
```

```
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

Modifications du filtre OTV requises en raison d'une défaillance du site

Si un site tombe en panne, les filtres doivent être supprimés de l'OTV, car il n'est plus nécessaire de bloquer l'adresse MAC globale. Certaines configurations supplémentaires sont nécessaires.

Vous devez ajouter une entrée statique pour l'adresse MAC globale ASA sur le commutateur OTV dans le site qui est fonctionnel. Cette entrée permettra à l'OTV à l'autre extrémité d'ajouter ces entrées sur l'interface de superposition. Cette étape est nécessaire, car si le serveur et le client ont déjà l'entrée ARP pour l'ASA, ce qui est le cas pour les connexions existantes, ils n'enverront pas à nouveau l'ARP. Par conséquent, l'OTV n'aura pas la possibilité d'apprendre l'adresse MAC globale ASA dans sa table de transfert. Étant donné que l'OTV n'a pas l'adresse MAC globale dans sa table de transfert et que, conformément à sa conception, il ne diffusera pas de paquets de monodiffusion sur l'interface de superposition, il abandonnera les paquets de monodiffusion à l'adresse MAC globale du serveur, et les connexions existantes seront interrompues.

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

Lorsque l'autre site est restauré, vous devez ajouter de nouveau les filtres et supprimer cette entrée statique sur l'OTV. Il est très important d'effacer le tableau des adresses MAC dynamiques sur les deux OTV pour effacer l'entrée de superposition pour l'adresse MAC globale.

Effacement du tableau d'adresses MAC

Lorsqu'un site tombe en panne et qu'une entrée statique pour l'adresse MAC globale est ajoutée à l'OTV, vous devez laisser l'autre OTV apprendre l'adresse MAC globale sur l'interface de superposition. Une fois l'autre site rétabli, ces entrées doivent être effacées. Assurez-vous d'effacer la table d'adresses MAC pour vous assurer que l'OTV ne conserve aucune de ces entrées dans sa table de transfert.

```
cluster-N7k6-OTV# show mac address-table
```

```
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

Supervision du cache OTV ARP

Le service OTV gère un cache ARP pour mandataire ARP pour les adresses IP qu'il a apprises sur l'interface OTV.

```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

Exemples de mise en grappe inter-sites

Les exemples suivants montrent les déploiements de grappe pris en charge.

Exemple de mode de routage EtherChannel étendu avec des adresses MAC et IP propres au site

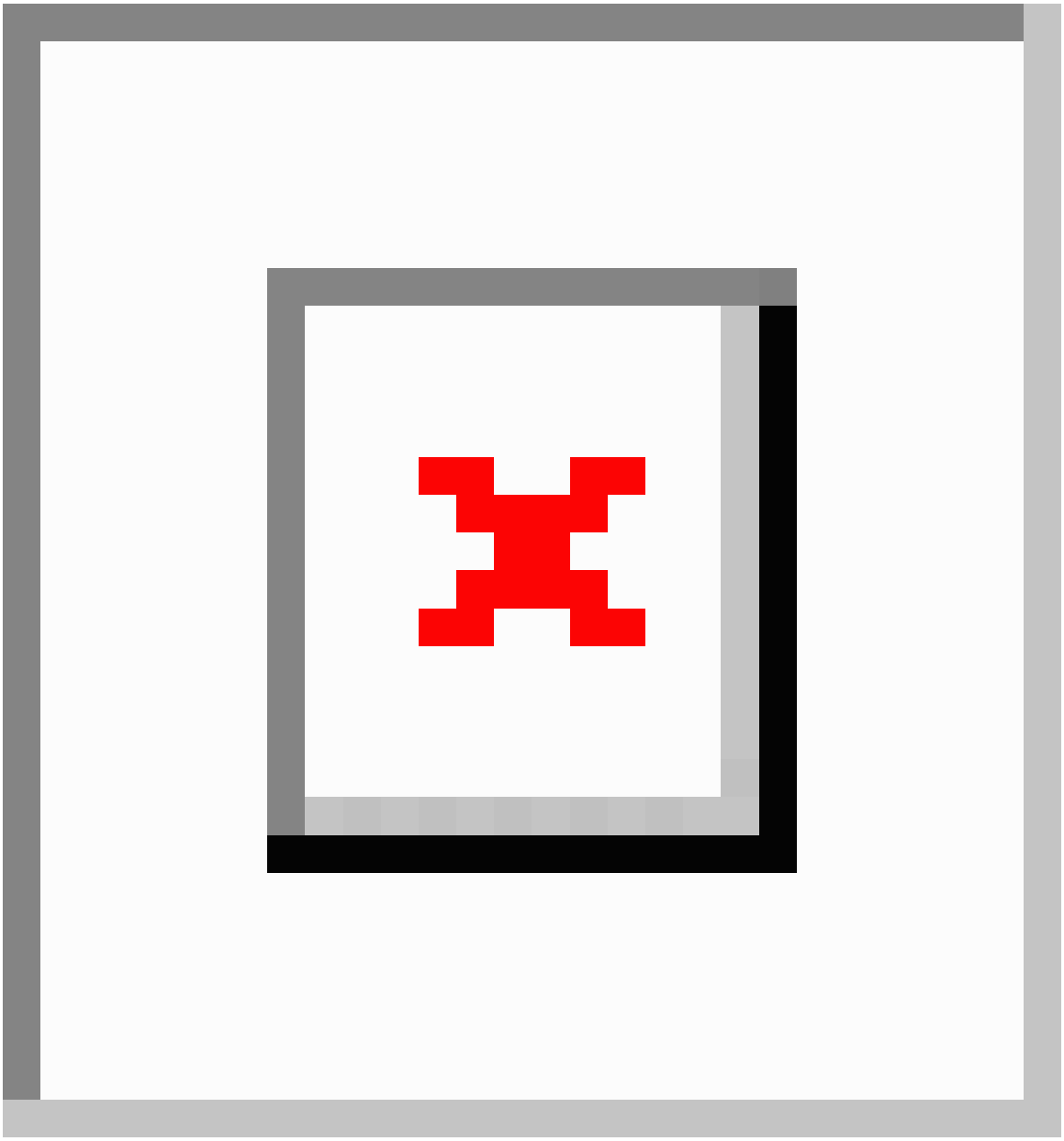
L'exemple suivant montre deux membres de la grappe dans chacun des deux centres de données, placés entre le routeur de passerelle et un réseau interne sur chaque site (insertion est-ouest). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs locaux en utilisant des EtherChannels étendus pour le réseau interne et externe. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Les VLAN de données sont étendus entre les sites à l'aide de la virtualisation du transport par superposition (OTV) (ou d'un outil similaire). Vous devez ajouter des filtres bloquant l'adresse MAC globale pour empêcher le trafic de traverser l'interface DCI vers l'autre site lorsqu'il est destiné à la grappe. Si les nœuds de la grappe d'un site deviennent inaccessibles, vous devez supprimer les filtres pour que le trafic puisse être dirigé vers les nœuds de la grappe de l'autre site. Vous devez utiliser les adresses VACL pour filtrer l'adresse MAC globale.Pour certains commutateurs, comme le Nexus avec la carte de ligne de la gamme F3, vous devez également utiliser l'inspection ARP pour bloquer les paquets ARP de l'adresse MAC globale. L'inspection ARP nécessite que vous définissiez à la fois l'adresse MAC et l'adresse IP du site sur l'ASA. Si vous configurez uniquement l'adresse MAC du site N'oubliez pas de désactiver l'inspection ARP.

La grappe sert de passerelle pour les réseaux internes. Le MAC virtuel global, qui est partagé sur tous les nœuds de la grappe, est utilisé uniquement pour recevoir des paquets. Les paquets sortants utilisent une adresse MAC spécifique au site pour chaque grappe de contrôleurs de domaine. Cette fonctionnalité empêche les commutateurs d'apprendre la même adresse MAC globale à partir des deux sites sur deux ports différents, ce qui entraîne une oscillation MAC; au lieu de cela, ils connaissent uniquement l'adresse MAC du site.

Dans ce scénario :

- Tous les paquets de sortie envoyés par la grappe utilisent l'adresse MAC du site et sont localisés dans le centre de données.
- Tous les paquets entrants vers la grappe sont envoyés à l'aide de l'adresse MAC globale, de sorte qu'ils peuvent être reçus par n'importe quel nœud des deux sites; les filtres de l'OTV localisent le trafic dans le centre de données.



Exemple intersites nord-sud de mode transparent de l'EtherChannel étendu

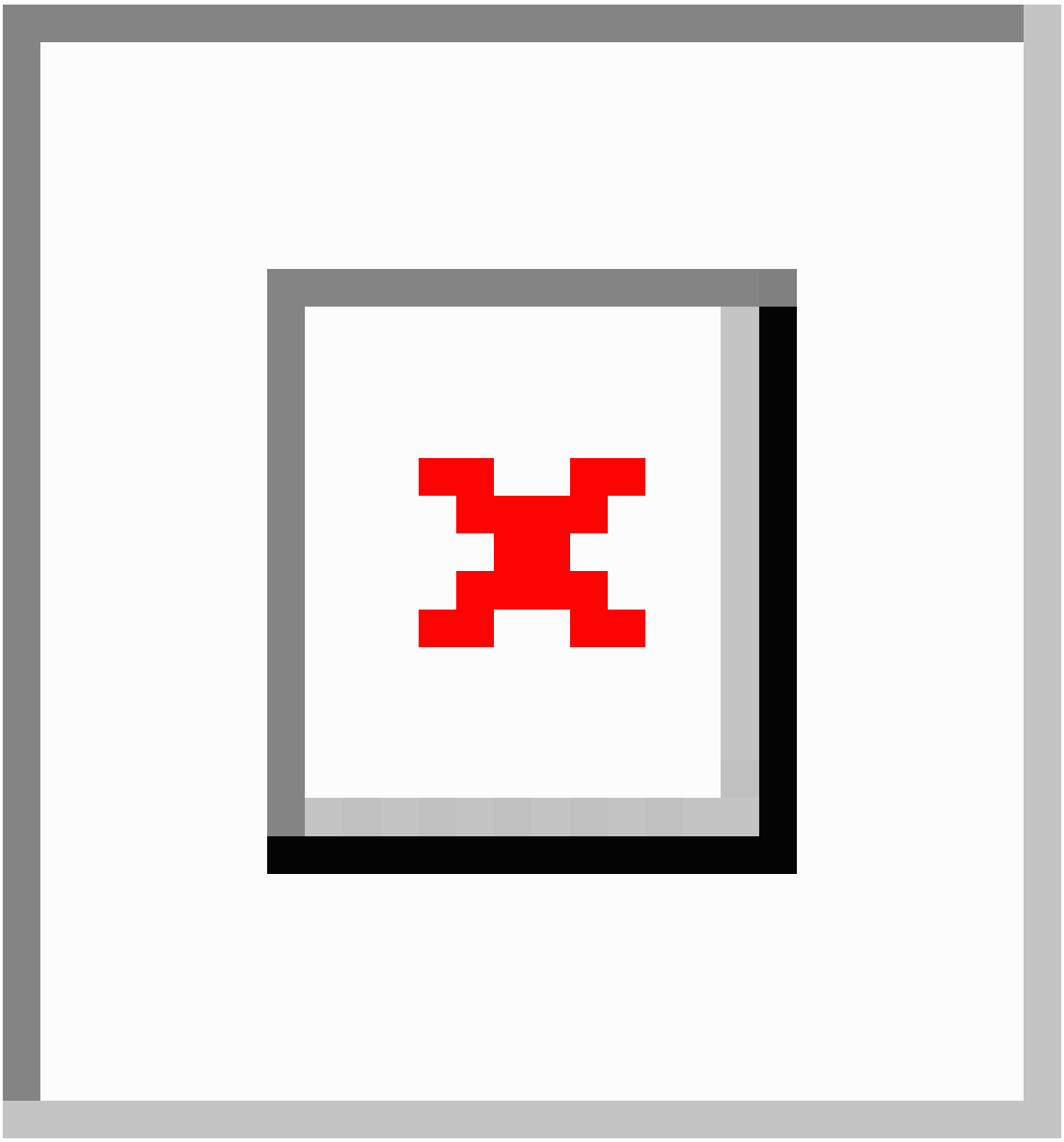
L'exemple suivant montre 2 membres de la grappe dans chacun des 2 centres de données placés entre les routeurs internes et externes (insertion nord-sud). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs

locaux en utilisant des EtherChannels étendus pour l'intérieur et l'extérieur. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Les routeurs internes et externes de chaque centre de données utilisent le protocole OSPF, qui est transmis par les périphériques ASA transparents. Contrairement aux MAC, les adresses IP des routeurs sont uniques sur tous les routeurs. En attribuant un routage à coût plus élevé sur l'interface DCI, le trafic reste dans chaque centre de données, sauf si tous les membres de la grappe d'un site donné tombent en panne. La voie de routage la moins dispendieuse qui traverse les ASA doit traverser le même groupe de ponts sur chaque site pour que la grappe puisse maintenir des connexions dissymétriques. En cas de défaillance de tous les membres de la grappe sur un site, le trafic passe de chaque routeur sur l'interface DCI aux membres de la grappe sur l'autre site.

La mise en œuvre des commutateurs sur chaque site peut inclure :

- VSS inter-sites, vPC, StackWise ou StackWise Virtual : dans ce scénario, vous installez un commutateur au centre de données 1, et l'autre au centre de données 2. Une option consiste à ce que les nœuds de la grappe de chaque centre de données se connectent uniquement au commutateur local, tandis que le trafic du commutateur redondant traverse le DCI. Dans ce cas, les connexions sont pour la plupart conservées localement à chaque centre de données. Vous pouvez éventuellement connecter chaque nœud aux deux commutateurs de la DCI si la DCI peut gérer le trafic supplémentaire. Dans ce cas, le trafic est réparti entre les centres de données, il est donc essentiel que l'interface DCI soit très robuste.
- Local VSS, vPC, StackWise ou StackWise Virtual sur chaque site : Pour une meilleure redondance des commutateurs, vous pouvez installer 2 paires de commutateurs redondants distincts sur chaque site. Dans ce cas, bien que les nœuds de la grappe aient toujours un EtherChannel étendu avec le châssis du centre de données 1 connecté uniquement aux deux commutateurs locaux et le châssis du centre de données 2 connecté à ces commutateurs locaux, l'EtherChannel étendu est essentiellement « divisé ». Chaque système de commutation local redondant voit l'EtherChannel étendu comme un EtherChannel local au site.

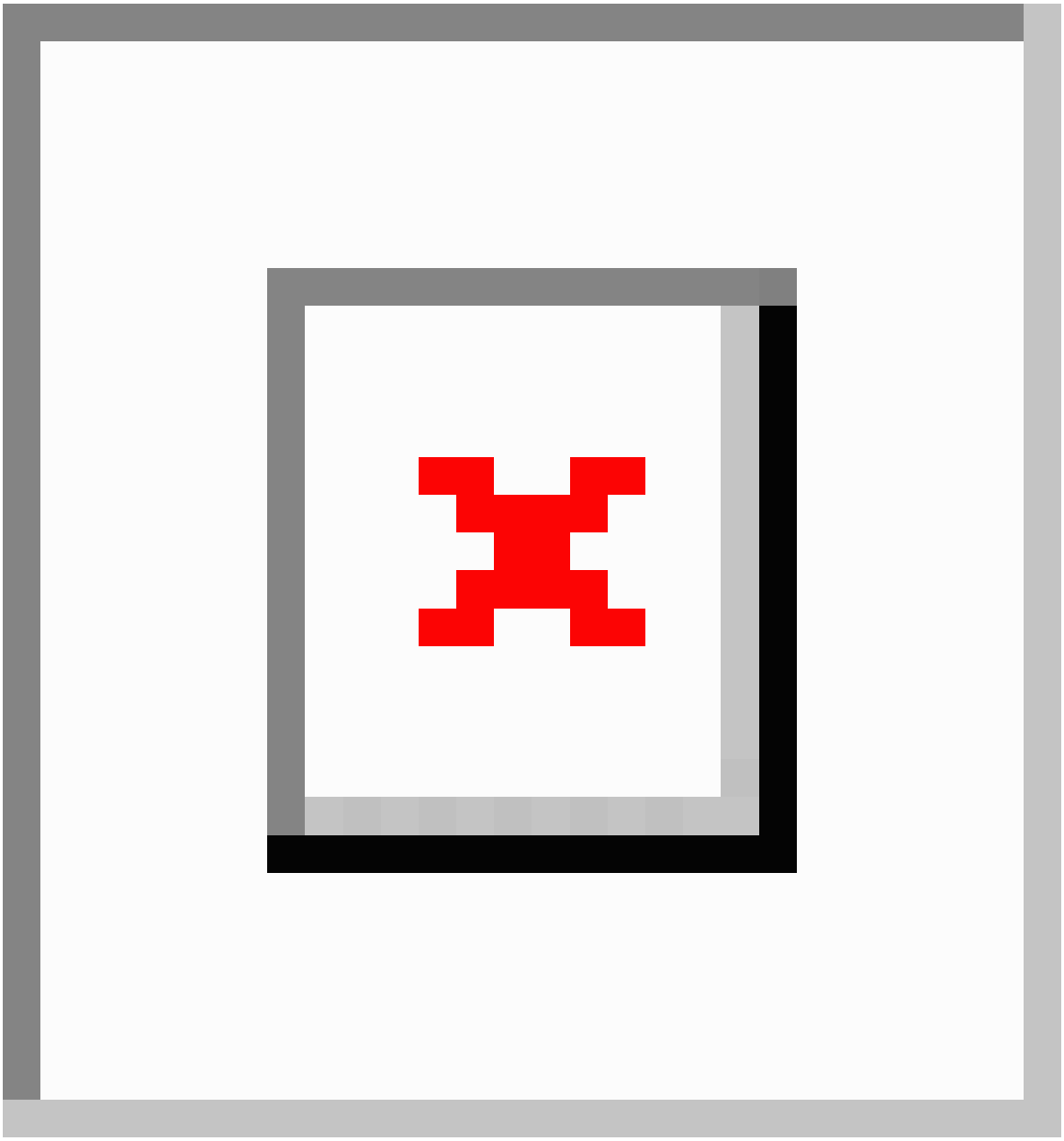


Exemple inter-sites est-ouest en mode transparent de l'EtherChannel étendu

L'exemple suivant montre deux membres de la grappe dans chacun des deux centres de données, placés entre le routeur de la passerelle et deux réseaux internes sur chaque site, le réseau d'applications et le réseau de base de données (insertion est-ouest). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs locaux au moyen d'EtherChannels étendus pour les réseaux App et DB à l'intérieur et à l'extérieur. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Le routeur de la passerelle de chaque site utilise un FHRP comme le HSRP pour fournir les mêmes adresses MAC virtuelles et IP de destination sur chaque site. Une bonne pratique pour éviter le basculement involontaire des adresses MAC consiste à ajouter de manière statique les adresses MAC réelles des routeurs de passerelle

au tableau d'adresses MAC de l'ASA. Sans ces entrées, si la passerelle du site 1 communique avec la passerelle du site 2, ce trafic pourrait passer par l'ASA et tenter d'atteindre le site 2 à partir de l'interface interne, ce qui poserait des problèmes. Les VLAN de données sont étendus entre les sites à l'aide de la virtualisation du transport par superposition (OTV) (ou d'un outil similaire). Vous devez ajouter des filtres pour empêcher le trafic de traverser l'interface DCI vers l'autre site lorsqu'il est destiné au routeur de la passerelle. Si le routeur de la passerelle d'un site devient inaccessible, vous devez supprimer les filtres pour que le trafic puisse être dirigé vers le routeur de la passerelle de l'autre site.



Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités et mise en grappe de l'ASA

Certaines fonctionnalités d'ASA ne sont pas prises en charge avec la mise en grappe d'ASA, et d'autres le sont uniquement sur le nœud de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités non prises en charge par la mise en grappe

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

- Fonctionnalités de communication unifiée qui reposent sur le mandataire TLS
- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Interfaces de tunnel virtuel (VTI)
- Les inspections d'application suivantes :
  - CTIQBE
  - H323, H225 et RAS
  - Intercommunication IPsec
  - MGCP
  - MMP
  - RTSP
  - SCCP (Skinny)
  - WAAS
  - WCCP
- Filtre de trafic de réseau de zombies
- Auto Update Server
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Équilibrage de la charge VPN
- Basculement
- Routage et pont intégrés
- Mode FIPS

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.



Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

- Ces inspections d'application sont prises en charge :
  - DCERPC et ESMTP
  - IM
  - NetBIOS et PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET et SUNRPC
  - TFTP
  - XDMCP
- Surveillance du routage statique
- Autorisation et authentification pour l'accès réseau La comptabilité est décentralisée.
- Services de filtrage
- VPN de site à site
- Traitement du protocole du plan de contrôle de multidiffusion IGMP (le transfert du plan de données est distribué dans la grappe)
- Traitement du protocole du plan de contrôle de multidiffusion PIM (le transfert du plan de données est distribué dans la grappe)
- Routage dynamique

Fonctionnalités appliquées aux nœuds individuels

Ces fonctionnalités sont appliquées à chaque nœud ASA, plutôt qu'à la grappe dans son ensemble ou au nœud de contrôle.

- QoS : la politique QoS est synchronisée dans la grappe dans le cadre de la duplication de la configuration. Cependant, la politique est appliquée sur chaque nœud indépendamment. Par exemple, si vous configurez le contrôle en sortie, les valeurs de débit de conformité et de rafale de conformité s'appliquent au trafic sortant d'un ASA particulier. Dans une grappe à 3 nœuds et avec le trafic réparti uniformément, le taux de conformité devient en fait trois fois supérieur au débit de la grappe.
- Détection des menaces : la détection des menaces fonctionne sur chaque nœud indépendamment; par exemple, les statistiques principales sont propres au nœud. La détection de l'analyse de port, par exemple, ne fonctionne pas, car l'analyse du trafic sera équilibrée entre tous les nœuds et un nœud ne verra pas tout le trafic.
- Gestion des ressources : la gestion des ressources en mode contexte multiple est appliquée séparément sur chaque nœud en fonction de l'utilisation locale.
- Trafic LISP : le trafic LISP sur le port UDP 4342 est inspecté par chaque nœud de réception, mais aucun directeur n'est affecté. Chaque nœud ajoute au tableau EID qui est partagé dans la grappe, mais le trafic LISP lui-même ne participe pas au partage de l'état de la grappe.

AAA pour l'accès réseau et la mise en grappe

L'AAA pour l'accès réseau comprend trois composants : l'authentification, l'autorisation et la gestion de comptes. L'authentification et l'autorisation sont mises en œuvre en tant que fonctionnalités centralisées sur le nœud de contrôle de mise en grappe avec la duplication des structures de données sur les nœuds de données de grappe. Si un nœud de contrôle est choisi, le nouveau nœud de contrôle disposera de toute l'information nécessaire pour continuer le fonctionnement ininterrompu des utilisateurs authentifiés établis et de leurs autorisations associées. Les délais d'inactivité et absolus pour l'authentification des utilisateurs sont conservés lorsqu'un changement de nœud de contrôle se produit.

La comptabilité est mise en œuvre en tant que fonctionnalité distribuée dans une grappe. La comptabilité est effectuée flux par flux, de sorte que le nœud de la grappe possédant un flux enverra les messages de démarrage et d'arrêt de comptabilité au serveur AAA lorsque la comptabilité est configurée pour un flux.

Paramètres de connexion et mise en grappe

Les limites de connexion s'appliquent à l'ensemble de la grappe (voir **Configuration** > **Firewall** > **Service Policy**, page). Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.
- Si vous utilisez l'AAA pour l'accès FTP, le flux du canal de contrôle est centralisé sur le nœud de contrôle.

Inspection ICMP et mise en grappe

Le flux des paquets d'erreurs ICMP et ICMP dans la grappe varie selon que l'inspection d'erreurs ICMP ou ICMP est activée ou non. Sans inspection ICMP, ICMP est un flux unidirectionnel et il n'y a pas de prise en charge de flux directeur. Avec l'inspection ICMP, le flux ICMP devient bidirectionnel et est soutenu par un flux directeur/de sauvegarde. L'une des différences avec un flux ICMP inspecté réside dans le traitement par le directeur du paquet transféré : le directeur transmettra le paquet de réponse d'écho ICMP au propriétaire du flux au lieu de retourner le paquet au transitaire.

Routage multidiffusion et mise en grappe

Routage multidiffusion en mode EtherChannel étendu

En mode EtherChannel étendu : l'unité de contrôle gère tous les paquets de routage de multidiffusion et les paquets de données jusqu'à ce que le transfert rapide soit établi. Une fois la connexion établie, chaque unité de données peut transférer des paquets de données en multidiffusion.

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents périphériques dans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à un périphérique qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe.

Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Routage et mise en grappe dynamiques

Cette section décrit comment utiliser le routage dynamique avec la mise en grappe.

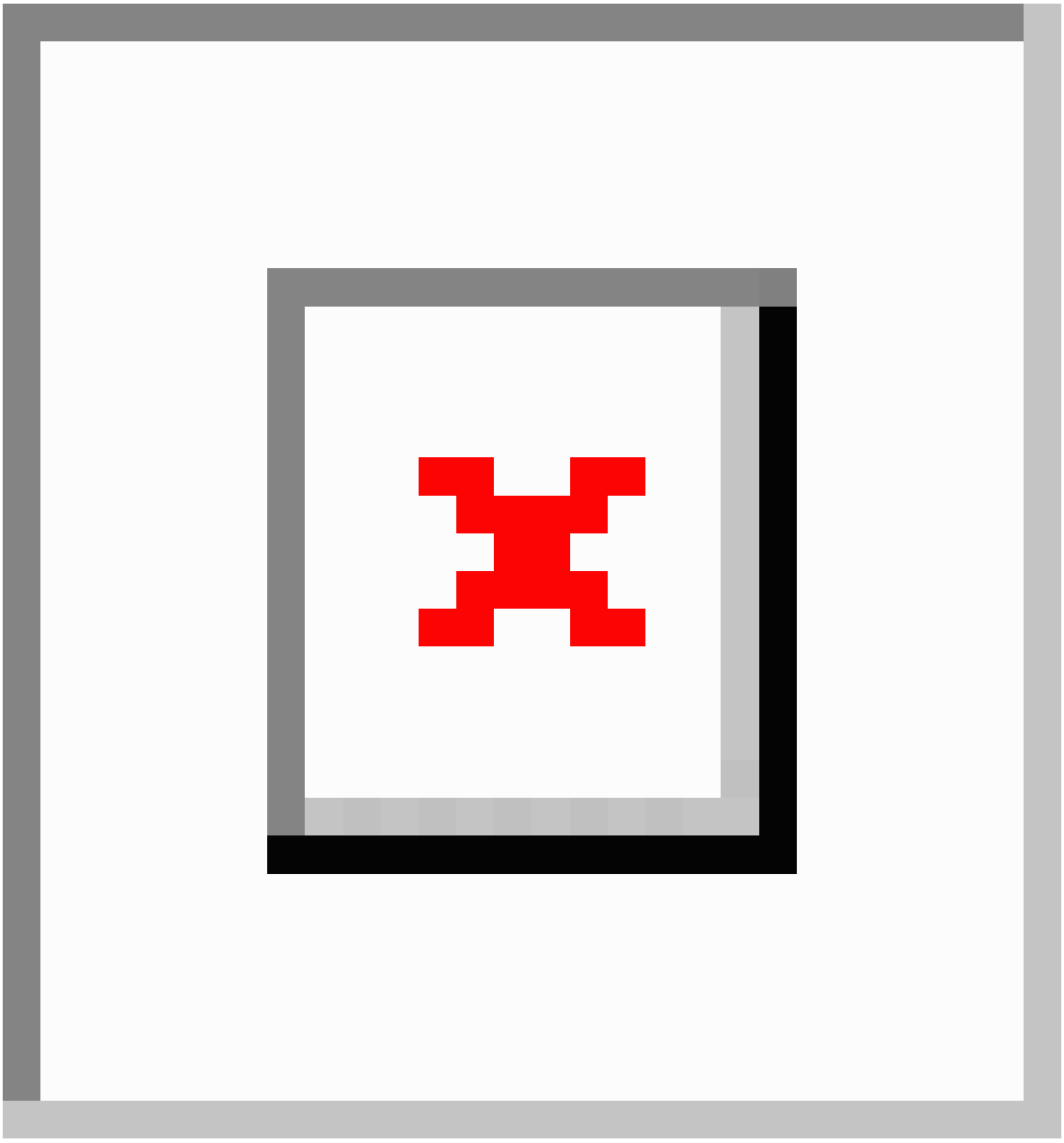
Routage dynamique en mode EtherChannel étendu

Le processus de routage ne s'exécute que sur le nœud de contrôle, et les routes sont apprises par le nœud de contrôle et répliquées sur les nœuds de données. Si un paquet de routage arrive à un nœud de données, il est redirigé vers le nœud de contrôle.



Remarque IS-IS n'est pas pris en charge en mode EtherChannel étendu.

Illustration 60 : Routage dynamique en mode EtherChannel étendu



Une fois que le nœud de données a appris les routes du nœud de contrôle, chaque nœud prend des décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée du nœud de contrôle avec les nœuds de données. S'il y a basculement du nœud de contrôle, le routeur voisin détectera un redémarrage; le basculement n'est pas transparent. Le processus OSPF choisit une adresse IP comme ID de routeur. Bien que cela ne soit pas obligatoire, vous pouvez attribuer un ID de routeur statique pour vous assurer qu'un ID de routeur cohérent est utilisé dans la grappe. Consultez la fonctionnalité de transfert sans arrêt OSPF pour gérer l'interruption.

SCTP et mise en grappe

Une association SCTP peut être créée sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses connexions multi-hébergement doivent résider sur le même nœud.

Inspection SIP et mise en grappe

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

La configuration du mandataire TLS n'est pas prise en charge.

SNMP et mise en grappe

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud.Vous devez les rajouter sur le nœud de contrôle pour forcer les utilisateurs à se reproduire vers le nouveau nœud, ou directement sur le nœud de données.

STUN et mise en grappe

L'inspection STUN est prise en charge dans les modes de basculement et de grappe, car les sténopés sont dupliqués. Cependant, l'ID de transaction n'est pas répliqué sur les nœuds. Dans le cas où un nœud tombe en panne après avoir reçu une demande STUN et qu'un autre nœud a reçu la réponse STUN, la réponse STUN sera abandonnée.

Syslog, NetFlow et mise en grappe

Syslog, NetFlow et la mise en grappe constituent une configuration de gestion de réseau qui permet la journalisation et la surveillance des flux dans les environnements réseau en grappe.

- Syslog : chaque nœud de la grappe génère ses propres messages de journal système. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.
- NetFlow : chaque nœud de la grappe génère son propre flux NetFlow. Le collecteur NetFlow peut traiter chaque appareil ASA uniquement comme un exportateur NetFlow distinct.

Cisco TrustSec et la mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

VPN et mise en grappe

Le VPN de site à site est une fonctionnalité centralisée; seul le nœud de contrôle prend en charge les connexions VPN.



Remarque L'accès VPN à distance n'est pas pris en charge avec la mise en grappe.

La fonctionnalité VPN est limitée au nœud de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si le nœud de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les utilisateurs de VPN verront une perturbation de service. Lorsqu'un nouveau nœud de contrôle est choisi, vous devez rétablir les connexions VPN.

Lorsque vous connectez un tunnel VPN à une adresse EtherChannel étendu, les connexions sont automatiquement transférées au nœud de contrôle.

Les clés et les certificats liés au VPN sont répliqués sur tous les nœuds.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Calcul du débit

Par exemple, si votre modèle peut gérer environ 10 Gbit/s de trafic lorsqu'il est exécuté seul, pour une grappe de 8 unités, le débit combiné maximal sera d'environ 80 % de 80 Gbit/s (8 unités x 10 Gbit/s) : 64 Gbit/s.

Élection du nœud de contrôle

process_summary

Les composants clés concernés dans le processus d'élection du nœud de contrôle sont les suivants :

- Nœuds de grappe : communiquent par la liaison de commande de grappe et participent au processus d'élection
- Demandes d'élection : diffusées toutes les 3 secondes par les nœuds lorsque la mise en grappe est activée
- Valeurs de priorité : définies entre 1 et 100, où 1 correspond à la priorité la plus élevée
- Nœud de contrôle : le nœud choisi qui coordonne les opérations de la grappe

process_workflow

Ces étapes décrivent comment les nœuds de la grappe élisent un nœud de contrôle :

1. Lorsque la mise en grappe est activée pour un nœud (ou lorsque celui-ci démarre pour la première fois alors que la mise en grappe est déjà activée), le nœud diffuse une demande d'élection toutes les 3 secondes.

2. Tout autre nœud ayant une priorité plus élevée répond à la demande d'élection. La priorité est comprise entre 1 et 100, 1 représentant la priorité la plus élevée.
3. Si, après 45 secondes, un nœud ne reçoit pas de réponse d'un autre nœud de priorité plus élevée, il devient le nœud de contrôle.

Remarque Si plusieurs nœuds sont à égalité pour la priorité la plus élevée, le nom du nœud de la grappe, suivi du numéro de série, est utilisé pour déterminer le nœud de contrôle.

4. Si un nœud rejoint ultérieurement la grappe avec une priorité plus élevée, il ne devient pas automatiquement le nœud de contrôle. Le nœud de contrôle existant conserve toujours son rôle, sauf s'il cesse de répondre, auquel cas un nouveau nœud de contrôle est élu.
5. Dans un scénario de « split brain », où plusieurs nœuds de contrôle sont temporairement présents, le nœud ayant la priorité la plus élevée conserve son rôle tandis que les autres nœuds reprennent leur rôle de nœud de données.

Remarque Vous pouvez forcer manuellement un nœud à devenir le nœud de contrôle. Pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Haute accessibilité au sein des grappes

La mise en grappe assure une disponibilité élevée en surveillant l'intégrité des nœuds et de l'interface et en reproduisant les états de la connexion entre les nœuds.

Supervision de l'intégrité du nœud

Chaque nœud envoie périodiquement un paquet de diffusion heartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet heartbeat ou autre paquet d'un nœud de données au cours du délai d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est élu parmi les nœuds restants.

Scénario de déconnexion cérébrale

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle.

Supervision des interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles désignées utilisées et signale les modifications d'état au nœud de contrôle.

- **Spanned EtherChannel** (EtherChannel étendu) : utilise le protocole cLACP (cluster Link Aggregation Control Protocol). Chaque nœud surveille l'état de la liaison et les messages du protocole cLACP pour déterminer si le port est toujours actif dans l'EtherChannel. L'état est signalé au nœud de contrôle.

Lorsque vous activez la surveillance de l'intégrité, toutes les interfaces physiques (y compris les interfaces EtherChannel principales) sont surveillées par défaut; vous pouvez éventuellement désactiver la surveillance par interface. Seules les interfaces nommées peuvent être surveillées. Par exemple, l'EtherChannel désigné doit échouer pour être considéré comme en échec, ce qui signifie que tous les ports membres d'un EtherChannel ne doivent pas déclencher la suppression de la grappe (selon le paramètre minimal de groupement de ports).

Un nœud est supprimé de la grappe en cas de défaillance de ses interfaces surveillées. Le délai avant que ASA ne supprime un membre de la grappe dépend dépend du fait que le nœud est un membre établi ou en train de se joindre à la grappe. si l'interface est en panne sur un membre établi, l'ASA supprime le membre après 9 secondes. L'ASA ne surveille pas les interfaces pendant les 90 premières secondes où un nœud rejoint la grappe. Les changements d'état de l'interface pendant cette période n'entraîneront pas le retrait de l'ASA de la grappe. Pour les non-EtherChannels, le nœud est supprimé après 500 ms, quel que soit l'état membre.

État après l'échec

Lorsqu'un nœud de la grappe tombe en panne, les connexions hébergées par ce nœud sont transférées en toute transparence vers d'autres nœuds; Les renseignements d'état sur les flux de trafic sont partagés sur la liaison de commande de grappe du nœud de contrôle.

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

Le périphérique tente automatiquement de rejoindre la grappe, selon l'événement de défaillance.

Remarque Lorsque le périphérique devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont désactivées ; seule l'interface de gestion peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe, l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Rejoindre la grappe

Après le retrait d'un nœud de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : l'ASA essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment. Ce comportement est configurable.

- Échec de l'interface de données : l'ASA tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'ASA désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe. Ce comportement est configurable.
- Nœud en échec : si le nœud a été supprimé de la grappe en raison d'un échec de vérification de l'intégrité du nœud, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que le nœud rejoindra la grappe au redémarrage, à condition que la liaison de commande de grappe soit active et que la mise en grappe soit toujours activée. L'ASA tente de rejoindre la grappe toutes les 5 secondes.
- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc. Un nœud tentera de rejoindre la grappe automatiquement aux intervalles suivants : 5 minutes, 10 minutes, puis 20 minutes. Ce comportement est configurable.

Consultez Configurer les paramètres de grappe ASA de base, à la page 396.

duplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 22 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
Tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	Comprend les règles AAA (uauth).
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	Non	—
VPN distribué (site à site)	Oui	La session de sauvegarde devient la session active, puis une nouvelle session de sauvegarde est créée.

Gestion des connexions par la grappe

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Ces rôles sont définis pour chaque connexion :

- **Owner** (Propriétaire) : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.
- **Backup Owner** (Propriétaire de sauvegarde) : nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

  Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis.

  Si vous activez la localisation du directeur pour la mise en grappe inter-sites, il existe deux rôles de propriétaire de la sauvegarde : le rôle de sauvegarde locale et de sauvegarde globale. Le propriétaire choisit toujours une sauvegarde locale sur le même site que lui (en fonction de l'ID du site). La sauvegarde globale peut se trouver sur n'importe quel site et peut même se trouver sur le même nœud que la sauvegarde locale. Le propriétaire envoie des informations sur l'état de la connexion aux deux sauvegardes.

  Si vous activez la redondance de sites et que le propriétaire de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La sauvegarde de châssis et la sauvegarde de site sont indépendantes. Par conséquent, dans certains cas, un flux comportera à la fois une sauvegarde de châssis et une sauvegarde de site.
- **Director** (Directeur) : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

  Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

Si vous activez la localisation de directeur pour la mise en grappe inter-sites, il y a deux rôles de directeur : le directeur local et le directeur global. Pour un paquet de nouveau flux, le membre de réception sélectionne le directeur local parmi les membres du site du membre de réception. Le directeur global peut se trouver sur n'importe quel site et peut être le même membre que le directeur local. En cas de défaillance du propriétaire d'origine et si la localisation s'applique, le directeur local choisit un nouveau propriétaire de connexion sur le site du directeur local.

Détails du hachage ICMP/ICMPv6 :

- Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
- Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
- Pour les autres paquets, les ports source et de destination sont à 0.

- **Forwarder** (Transitaire) : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Si vous activez la localisation de directeur, le transitaire interroge le directeur local lorsque la localisation s'applique. Le transitaire interroge le directeur global si le directeur local ne reconnaît pas le propriétaire, si la connexion appartient à un autre site ou si la localisation est contournée. Une requête de directeur intersite est le comportement attendu dans ces cas. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.



Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

- **Fragment Owner** (Propriétaire de fragment) : pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

Connexions par traduction d'adresse de port

Lorsqu'une connexion utilise la traduction d'adresses de port (PAT), le type de PAT (par session ou multisession) influence quel membre de la grappe devient propriétaire de la nouvelle connexion :

- PAT par session : le propriétaire est le nœud qui reçoit le paquet initial dans la connexion.

  Par défaut, le trafic TCP et DNS UDP utilise une PAT par session.

- PAT multisession : le propriétaire est toujours le nœud de contrôle. Si une connexion PAT multisession est initialement reçue par un nœud de données, le nœud de données transfère la connexion au nœud de contrôle.

  Par défaut, le trafic UDP (à l'exception du trafic UDP DNS) et ICMP utilise la PAT multisession. Ces connexions appartiennent donc toujours au nœud de contrôle.

Vous pouvez modifier les valeurs par défaut de PAT par session pour les protocoles TCP et UDP afin que les connexions à ces protocoles soient gérées par session ou multisession selon la configuration. Pour ICMP, vous ne pouvez pas modifier la PAT multisession par défaut. Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

Nouvelle propriété de connexion

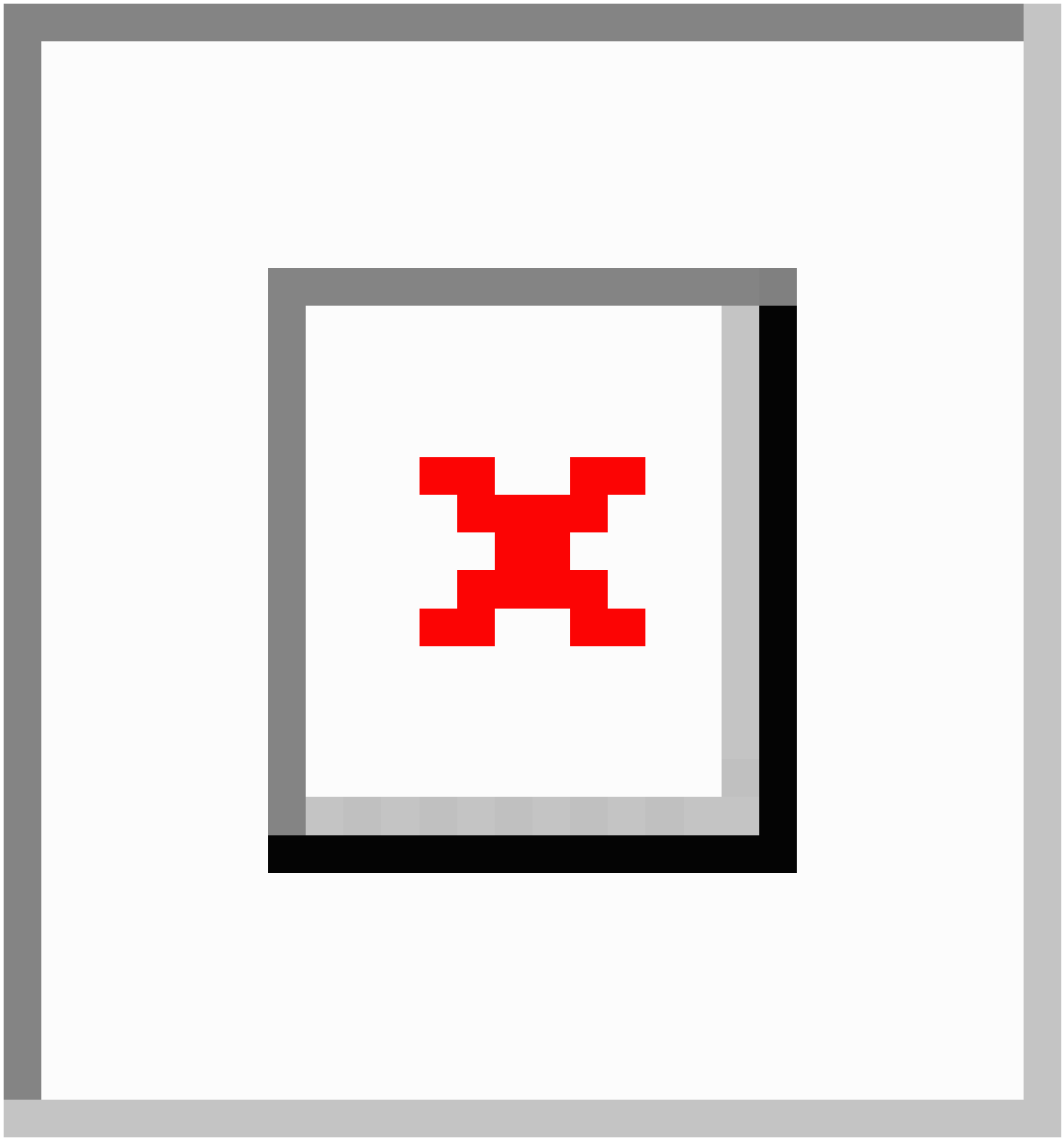
Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Pour de meilleures performances, un bon équilibrage de la charge externe est nécessaire pour que les deux directions d'un flux arrivent au même nœud et pour que les flux soient répartis uniformément entre les nœuds. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

process_summary

L'exemple suivant montre l'établissement d'une nouvelle connexion.

process_workflow



1. Le paquet SYN provient du client et est livré à un périphérique (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un périphérique différent (selon la méthode d'équilibrage de la charge). Ce périphérique est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.

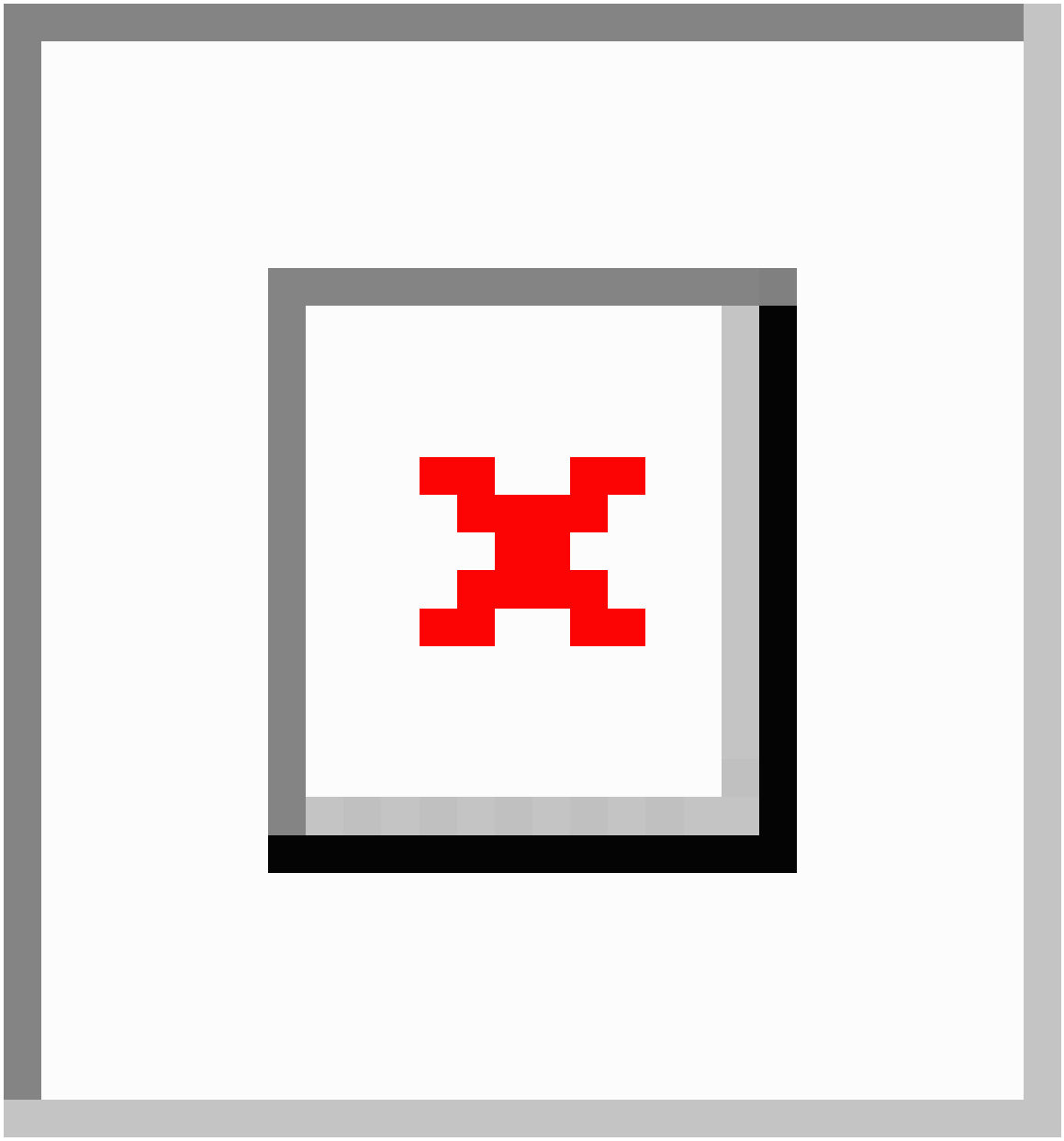
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.
5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.
7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

process_summary

L'exemple suivant montre l'établissement d'une nouvelle connexion.

process_workflow



1. Le premier paquet UDP provient du client et est remis à un périphérique (selon la méthode d'équilibrage de la charge).
2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.

6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.
8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Rééquilibrage des nouvelles connexions TCP dans la grappe

Si les capacités d'équilibrage de charges des routeurs en amont ou en aval entraînent une répartition non équilibrée des flux, vous pouvez configurer un rééquilibrage des nouvelles connexions afin que les nœuds ayant le plus de nouvelles connexions par seconde redirigent les nouveaux flux TCP vers d'autres nœuds. Aucun flux existant ne sera déplacé vers d'autres nœuds.

Comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal.

Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

Historique de la mise en grappe d'ASA pour le Secure Firewall

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
VPN site à site distribué avec mise en grappe sur le modèle Cisco Secure Firewall 4200	9.23(1)	Une grappe ASA sur le modèle Cisco Secure Firewall 4200 prend en charge le VPN de site à site en mode distribué. Le mode distribué permet d'avoir de nombreuses connexions VPN IPsec IKEv2 de site à site réparties sur les membres d'une grappe ASA, pas seulement sur le nœud de contrôle (comme en mode centralisé). Cela étend considérablement la prise en charge des VPN au-delà des capacités VPN centralisées et offre une haute disponibilité. Écrans nouveaux ou modifiés : **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > ASA Cluster (Grappe ASA) > VPN Cluster Summary (Résumé de la grappe VPN)** **Monitoring (Supervision) > VPN > VPN Statistics (Statistiques de VPN) > Sessions** **Configuration > Device Management (Gestion des périphériques) > High Availablility and Scalability (Haute disponibilité et évolutivité) > ASA Cluster (Grappe ASA)** **Wizards (Assistants) > Site-to-Site (Site à site)** **Monitoring (Supervision) > VPN > VPN Statistics (Statistiques de VPN) > Sessions** **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > ASA Cluster (Grappe ASA) > VPN Cluster Summary (Résumé de la grappe VPN)** **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > ASA Cluster (Grappe ASA) > System Resource Graphs (Graphique de ressources du système) > CPU/Memory (Processeur/mémoire)** **Monitoring (Supervision) > Logging (Journalisation) > Real-Time Log Viewer (Visionneuse de journal en temps réel)**
Suppression des propos tendancieux	9.19(1)	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
La prise en charge de la mise en grappe sur le pare-feu Secure Firewall 3100 a été introduite	9.17(1)	Vous pouvez mettre en grappe jusqu'à 8 nœuds Secure Firewall 3100 en mode EtherChannel étendu.



CHAPITRE 13

Grappe ASA pour le Firepower 4100/9300

La mise en grappe vous permet de regrouper plusieurs Châssis Firepower 4100/9300 en un seul périphérique logique. La série Châssis Firepower 4100/9300 comprend les Firepower 9300 et Firepower 4100. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités non prises en charge par la mise en grappe, à la page 518.

- À propos de la mise en grappe sur les châssis Firepower 4100/9300, à la page 451
- Exigences et conditions préalables à la mise en grappe sur Châssis Firepower 4100/9300 , à la page 459
- Licences pour la mise en grappe sur le Châssis Firepower 4100/9300 , à la page 461
- Lignes directrices et limites de la mise en grappe, à la page 462
- Configurer la mise en grappe sur le Châssis Firepower 4100/9300 , à la page 467
- FXOS : supprimer un nœud de la grappe, à la page 495
- ASA : Gérer les membres de la grappe, à la page 496
- ASA : supervision de la grappe ASA sur le Châssis Firepower 4100/9300 , à la page 501
- Dépannage du VPN S2S distribué, à la page 503
- Exemples de mise en grappe d'ASA, à la page 504
- Référence pour la mise en grappe, à la page 518
- Historique de la mise en grappe d'ASA sur le Firepower 4100/9300, à la page 537

À propos de la mise en grappe sur les châssis Firepower 4100/9300

Lorsque vous déployez une grappe sur le Châssis Firepower 4100/9300 , elle effectue les opérations suivantes :

- crée une *liaison de commande de grappe* (par défaut, le canal de port 48) pour la communication de nœud à nœud.

  Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, ce lien utilise le fond de panier Firepower 9300 pour les communications de la grappe.

Pour la mise en grappe avec plusieurs châssis, vous devez affecter manuellement une ou plusieurs interfaces physiques à cet EtherChannel pour les communications entre les châssis.

- Crée la configuration de démarrage de grappe dans l'application.

  Lorsque vous déployez la grappe, le superviseur de châssis envoie une configuration de démarrage minimale à chaque unité, qui comprend le nom de la grappe, l'interface de liaison de commande de grappe et d'autres paramètres de la grappe. Certaines parties de la configuration de démarrage peuvent être configurées par l'utilisateur dans l'application si vous souhaitez personnaliser votre environnement de mise en grappe.

- Affecte des interfaces de données à la grappe en tant *qu'interfaces étendues*.

  Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, les interfaces étendues ne se limitent pas aux EtherChannels, comme c'est le cas pour la mise en grappe avec plusieurs châssis. Le superviseur Firepower 9300 utilise la technologie EtherChannel en interne pour équilibrer la charge du trafic vers plusieurs modules sur une interface partagée, de sorte que tout type d'interface de données fonctionne pour le mode étendu. Pour la mise en grappe avec plusieurs châssis, vous devez utiliser des EtherChannels étendus pour toutes les interfaces de données.

Remarque Les interfaces individuelles ne sont pas prises en charge, à l'exception d'une interface de gestion.

- Attribue une interface de gestion à toutes les unités de la grappe.

Voir l'une des sections suivantes pour plus d'informations sur la mise en grappe.

Configuration du démarrage

Lorsque vous déployez la grappe, le superviseur de châssis Firepower 4100/9300 envoie une configuration de démarrage minimale à chaque unité, qui comprend le nom de la grappe, l'interface de liaison de commande de grappe et d'autres paramètres de la grappe. Certaines parties de la configuration de démarrage sont configurables par l'utilisateur si vous souhaitez personnaliser votre environnement de mise en grappe.

Membres de la grappe

Les membres de la grappe collaborent pour partager la politique de sécurité et les flux de trafic.

L'unité de **contrôle** est l'un des membres de la grappe. L'unité de contrôle est déterminée automatiquement. Tous les autres membres sont des unités de **données**.

Vous devez effectuer toute la configuration sur l'unité de contrôle uniquement; la configuration est ensuite reproduite dans les unités de données.

Certaines fonctionnalités ne sont pas évolutives dans une grappe, et l'unité de contrôle gère tout le trafic pour ces fonctionnalités. Voir Fonctionnalités centralisées pour la mise en grappe, à la page 519.

Liaison de commande de grappe

La liaison de commande de grappe est un EtherChannel (canal de port 48) pour la communication d'unité à unité. Pour la mise en grappe intra-châssis, cette liaison utilise le fond de panier Firepower 9300 pour les communications de la grappe. Pour la mise en grappe inter-châssis, vous devez affecter manuellement une ou plusieurs interfaces physiques à cet EtherChannel sur le Châssis Firepower 4100/9300 pour les communications entre les châssis.

Dans le cas d'une grappe inter-châssis à deux châssis, ne connectez pas directement la liaison de commande de grappe d'un châssis à l'autre. Si vous connectez directement les interfaces, lorsqu'une unité tombe en panne, la liaison de commande de grappe tombe en panne, et donc l'unité intègre restante. Si vous connectez la liaison de commande de grappe par l'intermédiaire d'un commutateur, cette dernière reste active pour l'unité intègre.

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

Consultez les sections suivantes pour en savoir plus sur la liaison de commande de grappe.

Dimensionnement de la liaison de commande de grappe

Le trafic de liaison de commande de grappe est principalement composé de mises à jour d'état et de paquets transférés. Le volume de trafic varie à un moment donné sur la liaison de commande de grappe. La quantité de trafic transféré dépend de l'efficacité de l'équilibrage de la charge et de l'importance du trafic pour les fonctionnalités centralisées.

Par exemple :

- La NAT entraîne un mauvais équilibrage de la charge des connexions et la nécessité de rééquilibrer tout le trafic de retour vers les bonnes unités.
- L'AAA pour l'accès réseau est une fonctionnalité centralisée, de sorte que tout le trafic est acheminé à l'unité de contrôle.
- Lorsque les membres changent, la grappe doit rééquilibrer un grand nombre de connexions, utilisant ainsi temporairement une grande quantité de bande passante de la liaison de commande de grappe.

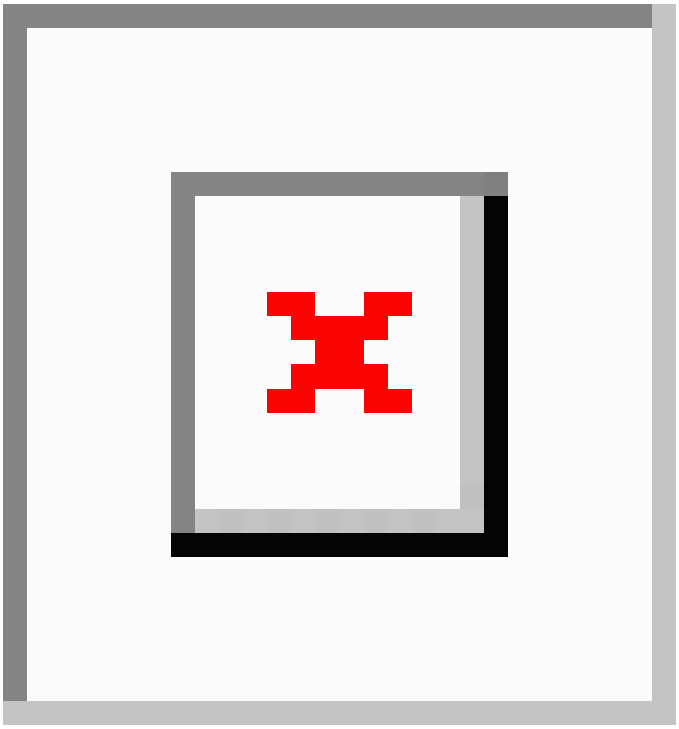
Une liaison de commande de grappe à bande passante plus élevée aide la grappe à converger plus rapidement lorsque les membres changent et empêche les goulots d'étranglement.

Remarque Si votre grappe génère un trafic asymétrique (rééquilibreur) important, vous devez augmenter la taille du lien de commande de grappe.

Redondance de la liaison de commande de la grappe

Nous vous recommandons d'utiliser un EtherChannel pour la liaison de commande de la grappe, afin de pouvoir transférer le trafic sur plusieurs liaisons de l'EtherChannel tout en assurant la redondance.

Le diagramme suivant montre comment utiliser un EtherChannel comme liaison de commande de la grappe dans un système de commutation virtuelle (VSS), un canal de port virtuel (vPC), un StackWise ou un environnement StackWise Virtual. Tous les liens de l'EtherChannel sont actifs. Lorsque le commutateur fait partie d'un système redondant, vous pouvez connecter des interfaces de pare-feu dans le même EtherChannel pour séparer les commutateurs du système redondant. Les interfaces des commutateurs sont membres de la même interface de canal de port EtherChannel, car les commutateurs distincts se comportent comme un seul commutateur. Notez qu'il s'agit d'un EtherChannel local au périphérique et non d'un EtherChannel étendu.



Fiabilité de la liaison de commande de grappe pour la mise en grappe

Pour assurer la fonctionnalité de la liaison de commande de grappe, vérifiez que le temps aller-retour (RTT) entre les unités est inférieur à 20 ms. Cette latence maximale améliore la compatibilité avec les membres de la grappe installés à différents sites géographiques. Pour vérifier votre latence, envoyez un message Ping sur la liaison de commande de grappe entre les unités.

La liaison de commande de grappe doit être fiable, sans paquets en désordre ou abandonnés; par exemple, pour un déploiement intersite, vous devez utiliser un lien dédié.

Réseau de liaison de commande de grappe

Le Châssis Firepower 4100/9300 génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID de châssis et de l'ID d'emplacement : 127.2.*chassis_id*.*slot-id*.Vous pouvez personnaliser cette adresse IP lorsque vous déployez la grappe. Le réseau de liaison de commande de grappe ne peut pas comprendre de routeurs entre les unités; seule la

commutation de couche 2 est autorisée. Pour le trafic intersites, Cisco recommande d'utiliser la virtualisation du transport par superposition (OTV).

Test de ping de la MTU de la liaison de commande de grappe

Utilisez les tests ping MTU de liaison de commande de grappe pour

- vérifier la compatibilité de l'unité de transfert vérifier la compatibilité de la MTU entre les nœuds de la grappe au cours du processus de jonction,
- utiliser des tests de fragmentation basés sur le ping pour confirmer que le chemin réseau prend en charge le traitement approprié des paquets, et
- permettre aux nœuds de rejoindre la grappe même si les tests échouent, tout en fournissant des messages de diagnostic pour le dépannage des incompatibilités de MTU.

Lorsqu'un nœud rejoint la grappe, le nœud de contrôle envoie un ping avec une charge utile d'une taille égale à deux fois la MTU. Ce processus teste la capacité du réseau à gérer la fragmentation des paquets, car la couche IP sous-jacente fragmentera les paquets qui dépassent la limite de MTU.

Un ping réussi confirme que le chemin réseau prend en charge une fragmentation appropriée et que la liaison de commande de grappe peut traiter de manière fiable le trafic avec la MTU configurée.

Si le ping échoue, affichez ces messages :

- **show cluster history**—`Événement : échec du test CCL MTU pour l'unité` *name*
- Console AVERTISSEMENT—`AVERTISSEMENT : L'unité` *name* `n'est pas accessible dans le test ICMP de trame étendue CCL, veuillez vérifier l'interface de grappe et la configuration MTU du commutateur.`

Même si le message ping échoue, le nœud est autorisé à rejoindre la grappe. Dans ce cas, vous devez résoudre la non-concordance de MTU dès que possible.

Interfaces de la grappe

Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, vous pouvez affecter des interfaces physiques ou des EtherChannels (également appelés canaux de port) à la grappe. Les interfaces affectées à la grappe sont des interfaces étendues qui équilibrent la charge du trafic entre tous les membres de la grappe.

Pour la mise en grappe avec plusieurs châssis, vous pouvez uniquement affecter des EtherChannels de données à la grappe. Ces EtherChannels étendus comprennent les mêmes interfaces membre sur chaque châssis; Sur le commutateur en amont, toutes ces interfaces sont incluses dans un seul EtherChannel, de sorte que le commutateur ne sache pas qu'il est connecté à plusieurs périphériques.

Les interfaces individuelles ne sont pas prises en charge, à l'exception d'une interface de gestion.

Connexion à un système de commutateurs redondants

Nous vous recommandons de connecter les EtherChannels à un système de commutation redondant tel qu'un VSS, vPC, StackWise ou un système virtuel StackWise pour assurer la redondance de vos interfaces.

Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

Gestion des grappes Cisco Secure Firewall ASA

L'un des avantages de l'utilisation de la mise en grappe ASA est la facilité de gestion. Cette section décrit comment gérer la grappe.

Réseau de gestion

Nous vous recommandons de connecter toutes les unités à un seul réseau de gestion. Ce réseau est distinct de la liaison de commande de grappe.

Interface de gestion

Vous devez affecter une interface de type gestion à la grappe. Cette interface est une interface individuelle spéciale, par opposition à une interface étendue. L'interface de gestion vous permet de vous connecter directement à chaque unité.

L'adresse IP de la grappe principale est une adresse fixe pour la grappe qui appartient toujours à l'unité de contrôle actuelle. Vous configurez également une plage d'adresses de sorte que chaque unité, y compris l'unité de contrôle actuelle, puisse utiliser une adresse locale de la plage. L'adresse IP de la grappe principale fournit un accès de gestion cohérent à une adresse; lorsqu'une unité de contrôle change, l'adresse IP de la grappe principale est déplacée vers la nouvelle unité de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente.

Par exemple, vous pouvez gérer la grappe en vous connectant à l'adresse IP de la grappe principale, qui est toujours associée à l'unité de contrôle actuelle. Pour gérer un membre, vous pouvez vous connecter à l'adresse IP locale.



Remarque Le trafic vers la boîte doit être acheminé vers l'adresse IP de gestion du nœud; le trafic vers la boîte n'est pas transféré sur la liaison de commande de grappe vers un autre nœud.

Pour le trafic de gestion sortant tel que TFTP ou syslog, chaque unité, y compris l'unité de contrôle, utilise l'adresse IP locale pour se connecter au serveur.

Gestion de l'unité de contrôle vs Gestion de l'unité de données

La gestion et la surveillance peuvent avoir lieu sur le nœud de contrôle. À partir du nœud de contrôle, vous pouvez vérifier les statistiques d'exécution, l'utilisation des ressources ou d'autres informations de surveillance sur tous les nœuds. Vous pouvez également transmettre une commande à tous les nœuds de la grappe et reproduire les messages de console des nœuds de données vers le nœud de contrôle.

Vous pouvez surveiller directement les nœuds de données si vous le souhaitez. Bien que cela soit également disponible à partir du nœud de contrôle, vous pouvez effectuer la gestion de fichiers sur les nœuds de données (y compris la sauvegarde de la configuration et la mise à jour des images). Les fonctions suivantes ne sont pas disponibles à partir du nœud de commande :

- Surveillance des statistiques propres à la grappe par nœud.
- Surveillance des journaux système par nœud (sauf pour les journaux système envoyés à la console lorsque la duplication de la console est activée).
- SNMP
- NetFlow

duplication de clé de chiffrement

Lorsque vous créez une clé de chiffrement sur le nœud de contrôle, la clé est répliquée sur tous les nœuds de données. Si vous avez une session SSH sur l'adresse IP de la grappe principale, vous serez déconnecté en cas de défaillance du nœud de contrôle. Le nouveau nœud de contrôle utilise la même clé pour les connexions SSH, de sorte que vous n'avez pas besoin de mettre à jour la clé d'hôte SSH mise en cache lorsque vous vous reconnectez au nouveau nœud de contrôle.

Incompatibilité d'adresse IP du certificat de connexion ASDM

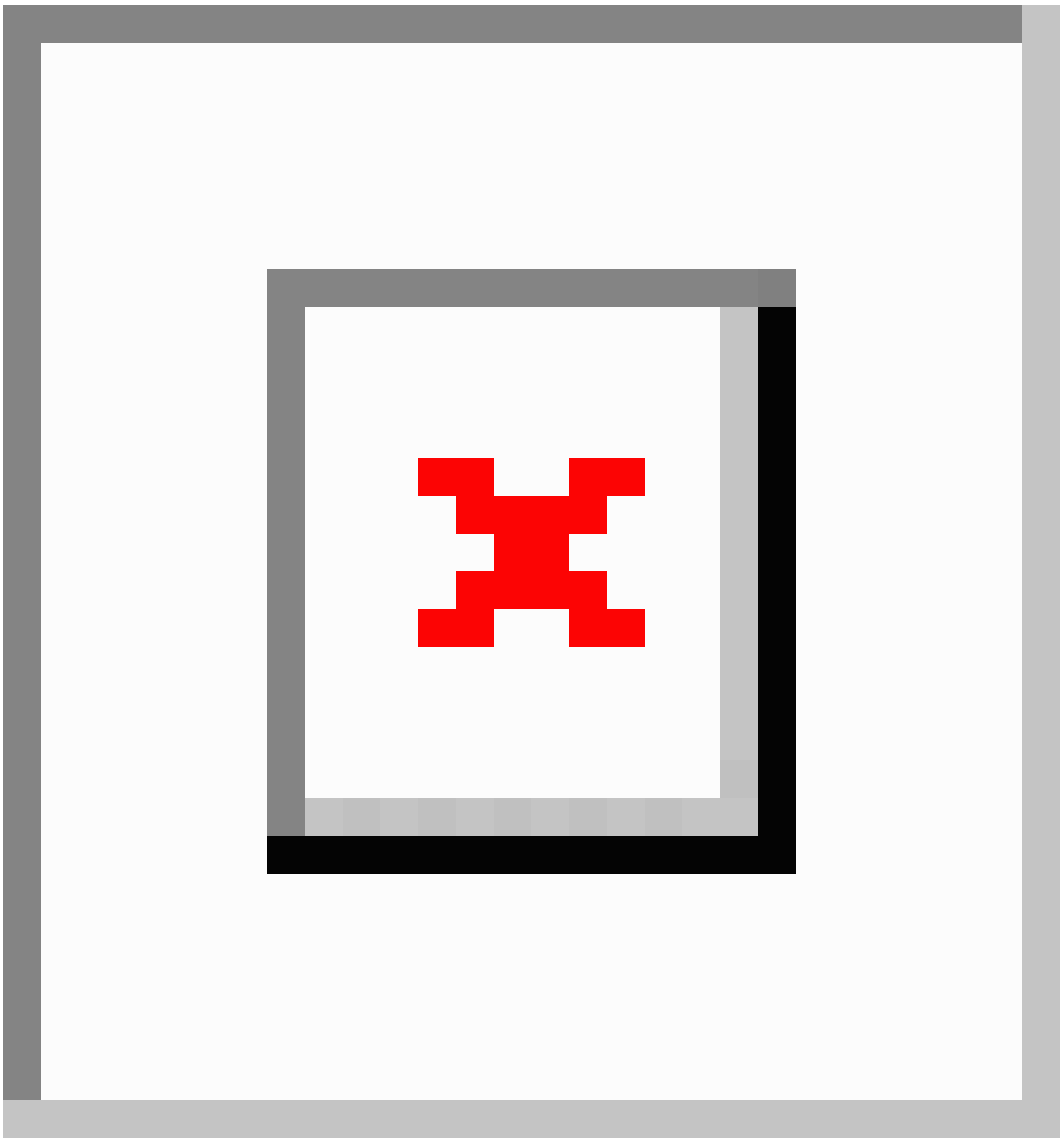
Par défaut, un certificat autosigné est utilisé pour la connexion ASDM en fonction de l'adresse IP locale. Si vous vous connectez à l'adresse IP de la grappe principale à l'aide d'ASDM, un message d'avertissement concernant une adresse IP non concordante peut s'afficher, car le certificat utilise l'adresse IP locale, et non l'adresse IP de la grappe principale. Vous pouvez ignorer le message et établir la connexion ASDM. Cependant, pour éviter ce type d'avertissement, vous pouvez inscrire un certificat qui contient l'adresse IP de la grappe principale et toutes les adresses IP locales de l'ensemble d'adresses IP. Vous pouvez ensuite utiliser ce certificat pour chaque membre de la grappe. Consultez https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html pour de plus amples renseignements.

EtherChannels étendus (recommandé)

Vous pouvez regrouper une ou plusieurs interfaces par châssis dans un EtherChannel qui s'étend sur tous les châssis de la grappe. L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal.

Un EtherChannel étendu peut être configuré dans les modes de pare-feu avec routage et transparent. En mode routé, l'EtherChannel est configuré comme une interface routée avec une seule adresse IP. En mode transparent, l'adresse IP est attribuée aux BVI, et non à l'interface du membre du groupe de ponts.

L'EtherChannel assure intrinsèquement l'équilibrage de la charge dans le cadre du fonctionnement de base.



Mise en grappe inter-sites

Pour les installations inter-sites, vous pouvez profiter de la mise en grappe d'ASA tant que vous suivez les lignes directrices recommandées.

Vous pouvez configurer chaque châssis de grappe pour qu'il appartienne à un ID de site distinct.

Les ID de site fonctionnent avec des adresses MAC et des adresses IPspécifiques au site . Les paquets qui sortent de la grappe utilisent une adresse MAC et une adresse IPpropres au site, tandis que les paquets reçus par la grappe utilisent une adresse MAC et une adresse IPglobales. Cette fonctionnalité empêche les commutateurs d'apprendre la même adresse MAC globale à partir des deux sites sur deux ports différents, ce qui entraîne une oscillation MAC; au lieu de cela, ils connaissent uniquement l'adresse MAC du site. Les adresses MAC et les adresses IP spécifiques au site sont prises en charge pour le mode routé qui utilise uniquement les EtherChannels étendus.

Les ID de site sont également utilisés pour permettre la mobilité de flux à l'aide de l'inspection LISP, la localisation du directeur pour améliorer les performances et réduire la latence aller-retour pour la mise en grappe inter-sites pour les centres de données, et la redondance des sites pour les connexions où un propriétaire de secours d'un flux se trouve toujours sur un autre site que celui du propriétaire.

Consultez les sections suivantes pour en savoir plus sur la mise en grappe inter-sites :

- Dimensionnement de l'interconnexion du centre de données : Exigences et conditions préalables à la mise en grappe sur Châssis Firepower 4100/9300 , à la page 459
- Lignes directrices inter-sites : Lignes directrices et limites de la mise en grappe, à la page 462
- Configurer la mobilité des flux de grappes : Configurer la mobilité des flux de grappes, à la page 485
- Activer la localisation du directeur : Configurer les paramètres de grappe ASA de base, à la page 479
- Activer la redondance de site : Configurer les paramètres de grappe ASA de base, à la page 479

Exigences et conditions préalables à la mise en grappe sur Châssis Firepower 4100/9300

Maximum d'unités de mise en grappe par modèle

- Firepower 4100 : 16 châssis
- Firepower 9300 : 16 modules. Par exemple, vous pouvez utiliser 1 module dans 16 châssis, ou 2 modules dans 8 châssis, ou toute combinaison qui fournit un maximum de 16 modules.

Exigences matérielles et logicielles pour la mise en grappe inter-châssis

Tous les châssis d'une grappe :

- : pour Firepower 4100 : tous les châssis doivent être du même modèle. Pour le périphérique Firepower 9300 : tous les modules de sécurité doivent être du même type. Par exemple, si vous utilisez la mise en grappe, tous les modules du périphérique Firepower 9300 doivent être des SM-40. Vous pouvez avoir différentes quantités de modules de sécurité installés dans chaque châssis, bien que tous les modules présents dans le châssis doivent appartenir à la grappe, y compris les logements vides.
- Doit exécuter FXOS et le logiciel d'application identiques, sauf au moment d'une mise à niveau d'image. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.
- Doit inclure la même configuration d'interface pour les interfaces que vous affectez à la grappe, comme la même interface de gestion, les mêmes EtherChannels, les interfaces actives, la vitesse et le duplex, etc. Vous pouvez utiliser différents types de modules de réseau sur le châssis tant que les capacités correspondent pour les mêmes ID d'interface et que les interfaces peuvent être groupées avec succès dans le même EtherChannel étendu. Notez que toutes les interfaces de données doivent être des EtherChannels dans des grappes à plusieurs châssis. Si vous modifiez les interfaces dans FXOS après avoir activé la mise en grappe (en ajoutant ou en supprimant des modules d'interface, ou en configurant EtherChannels, par exemple), vous effectuez les mêmes modifications sur chaque châssis, en commençant par les nœuds de données jusqu'au nœud de contrôle.Notez que si vous supprimez une interface dans FXOS, la configuration de l'ASA conserve les commandes correspondantes afin que vous puissiez

effectuer les ajustements nécessaires; la suppression d'une interface de la configuration peut avoir des effets importants. Vous pouvez supprimer manuellement l'ancienne configuration d'interface.

- Doit utiliser le même serveur NTP. Ne réglez pas l'heure manuellement.
- ASA : chaque châssis FXOS doit être enregistré auprès de l'autorité de licence ou du serveur satellite. Il n'y a pas de frais supplémentaires pour les nœuds de données. Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis. Pour Firewall Threat Defense, toutes les licences sont gérées par Firewall Management Center.

Exigences du commutateur

- Assurez-vous de terminer la configuration du commutateur et de connecter avec succès tous les canaux EtherChannels du châssis aux commutateurs avant de configurer la mise en grappe sur le Châssis Firepower 4100/9300 .
- Pour les caractéristiques de commutateur prises en charge, consultez Compatibilité Cisco FXOS.

dimensionnement de l'interconnexion du centre de données pour la mise en grappe inter-sites

Vous devez réserver la bande passante sur l'interconnexion des centres de données (DCI) pour un trafic de liaison de commande de grappe équivalent au calcul suivant :



Si le nombre de membres diffère sur chaque site, utilisez le plus grand nombre pour votre calcul. La bande passante minimale pour l'interface DCI ne doit pas être inférieure à la taille de la liaison de commande de grappe pour un membre.

Par exemple :

- Pour 4 membres sur 2 sites :
  - 4 membres de la grappe au total
  - 2 membres sur chaque site
  - Liaison de commande de grappe de 5 Gbit/s par membre

  Bande passante DCI réservée = 5 Gbit/s (2/2 x 5 Gbit/s).
- Pour 6 membres sur 3 sites, la taille augmente :
  - Six membres de la grappe au total
  - 3 membres sur le site 1, 2 membres sur le site 2 et 1 membre sur le site 3
  - Liaison de commande de grappe de 10 Gbit/s par membre

  Bande passante DCI réservée = 15 Gbit/s (3/2 x 10 Gbit/s).
- Pour 2 membres sur 2 sites :
  - 2 membres de la grappe au total
  - Un membre sur chaque site

- Liaison de commande de grappe de 10 Gbit/s par membre

Bande passante DCI réservée = 10 Gbit/s (1/2 x 10 Gbit/s = 5 Gbit/s, mais la bande passante minimale ne doit pas être inférieure à la taille de la liaison de commande de grappe (10 Gbit/s)).

Licences pour la mise en grappe sur le Châssis Firepower 4100/9300

Smart Software Manager standard et sur site

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence. Pour utiliser le cryptage renforcé et d'autres licences facultatives, chaque Châssis Firepower 4100/9300 doit être enregistré auprès de l'autorité de licence ou du serveur Smart Software Manager standard et sur site. Il n'y a pas de frais supplémentaires pour les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Lors de l'utilisation du jeton, chaque châssis doit avoir la même licence de chiffrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : seule l'unité de contrôle demande la licence Essentials au serveur et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.
- Contexte : seule l'unité de contrôle demande la licence de contexte au serveur. La licence Essentials comprend 10 contextes par défaut et est présente sur tous les membres de la grappe. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité de contrôle, sont combinées jusqu'à la limite de plateformes dans une licence de grappe agrégée. Par exemple :
  - Vous avez 6 modules Firepower 9300 dans la grappe. La licence Essentials comprend 10 contextes; pour 6 unités, ces licences ajoutent jusqu'à 60 contextes. Vous configurez une licence de 20 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 80 contextes. Comme la limite de plateformes pour un module est de 250, la licence combinée autorise un maximum de 250 contextes; les 80 contextes sont dans la limite. Par conséquent, vous pouvez configurer jusqu'à 80 contextes sur l'unité de contrôle; chaque unité de données aura également 80 contextes par la réplication de la configuration.
  - Vous avez 3 unités Firepower 4112 dans la grappe. La licence Essentials comprend 10 contextes; pour 3 unités, ces licences ajoutent jusqu'à 30 contextes. Vous configurez une licence de 250 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 280 contextes. Comme la limite de plateformes pour une unité est de 250, la licence combinée autorise un maximum de 250 contextes; les 280 contextes sont au-dessus de la limite. Par conséquent, vous ne pouvez configurer que 250 contextes sur l'unité de contrôle; chaque unité de données aura également 250 contextes par la réplication de la configuration. Dans ce cas, vous devez uniquement configurer la licence de contexte de l'unité de contrôle pour 220 contextes.

- Opérateur : requis pour le VPN S2S distribué. Cette licence est un droit par unité, et chaque unité demande sa propre licence au serveur.
- Cryptage renforcé (3DES) : pour un déploiement Cisco Smart Software Manager sur site antérieur à la version 2.3.0, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Cette licence est un droit par unité, et chaque unité demande sa propre licence au serveur.

Si une nouvelle unité de contrôle est choisie, la nouvelle unité de contrôle continue d'utiliser la licence agrégée. Elle utilise également la configuration de licence mise en mémoire cache pour demander à nouveau la licence de l'unité de contrôle. Lorsque l'ancienne unité de contrôle rejoint la grappe en tant qu'unité de données, elle libère le droit de licence de l'unité de contrôle. Avant que l'unité de données ne libère la licence, la licence de l'unité de contrôle peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La licence conservée est valide pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement d'autorisation toutes les 12 heures jusqu'à ce que la licence soit conforme. Vous devez éviter de modifier la configuration jusqu'à ce que les demandes de licences soient complètement traitées. Si une unité quitte la grappe, la configuration de contrôle mise en mémoire cache est supprimée, tandis que les droits par unité sont conservés. En particulier, vous devrez demander à nouveau la licence de contexte sur les unités qui ne sont pas des grappes.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer la mise en grappe.

Lignes directrices et limites de la mise en grappe

Commutateurs pour la mise en grappe

- Assurez-vous que les commutateurs connectés correspondent aux unités de transfert maximales MTU des interfaces de données et de l'interface de liaison de commande de grappe. Vous devez configurer la MTU de l'interface de la liaison de commande de grappe pour qu'elle soit au moins 100 octets supérieure à la MTU de l'interface de données. Assurez-vous donc de configurer le commutateur de connexion de la liaison de commande de grappe correctement. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe. De plus, nous ne conseillons pas de définir la MTU de la liaison de commande de grappe entre 2 561 et 8 362. En raison de la gestion du groupe de blocs, cette taille de MTU n'est pas optimale pour le fonctionnement du système.
- Pour les systèmes Cisco IOS XR, si vous souhaitez définir une MTU autre que celle par défaut, définissez la MTU de l'interface IOS XR sur 14 octets au-dessus de la MTU du périphérique de la grappe. Sinon, les tentatives d'homologation de contiguïté OSPF peuvent échouer, sauf si l'option **mtu-ignore** est utilisée. Notez que la MTU du périphérique de grappe doit correspondre à la MTU *IPv4* d'IOS XR. Cet ajustement n'est pas nécessaire pour les commutateurs Cisco Catalyst et Cisco Nexus.
- Sur le ou les commutateurs pour les interfaces de liaison de commande de grappe, vous pouvez éventuellement activer Spanning Tree PortFast sur les ports de commutateur connectés à l'unité de la grappe pour accélérer le processus de jonction des nouvelles unités.

- Sur le commutateur, nous vous conseillons d'utiliser l'un des algorithmes d'équilibrage de charges EtherChannel suivants : **source-dest-ip** or **src-dst-mixed-ip-port** (reportez-vous à la commande **port-channel load-balance** de Cisco Nexus OS et Cisco IOS-XE). N'utilisez pas de mot clé **vlan** dans l'algorithme d'équilibrage de charge, car cela pourrait entraîner une répartition inégale du trafic vers les périphériques d'une grappe. *Ne modifiez pas* l'algorithme d'équilibrage de charge par défaut sur le périphérique de la grappe.
- Si vous modifiez l'algorithme d'équilibrage de charge de l'EtherChannel sur le commutateur, l'interface EtherChannel du commutateur arrête temporairement de transférer le trafic et le protocole Spanning Tree redémarre. Il faudra attendre un certain temps avant que le trafic ne redevienne fluide.
- Les commutateurs sur le chemin de la liaison de commande de grappe ne doivent pas vérifier la somme de contrôle L4. Le trafic redirigé sur la liaison de commande de grappe n'a pas une somme de contrôle L4 correcte. Les commutateurs qui vérifient la somme de contrôle L4 pourraient entraîner l'abandon du trafic.
- Le temps d'arrêt du groupage du canal de port ne doit pas dépasser l'intervalle Keepalive configuré.
- Sur les EtherChannels de 2e génération, l'algorithme de distribution de hachage par défaut est adaptatif. Pour éviter le trafic symétrique dans une conception VSS, modifiez l'algorithme de hachage sur le canal de port connecté au périphérique de la grappe à fixe :

  router(config)# **port-channel** *id* **hash-distribution fixed**

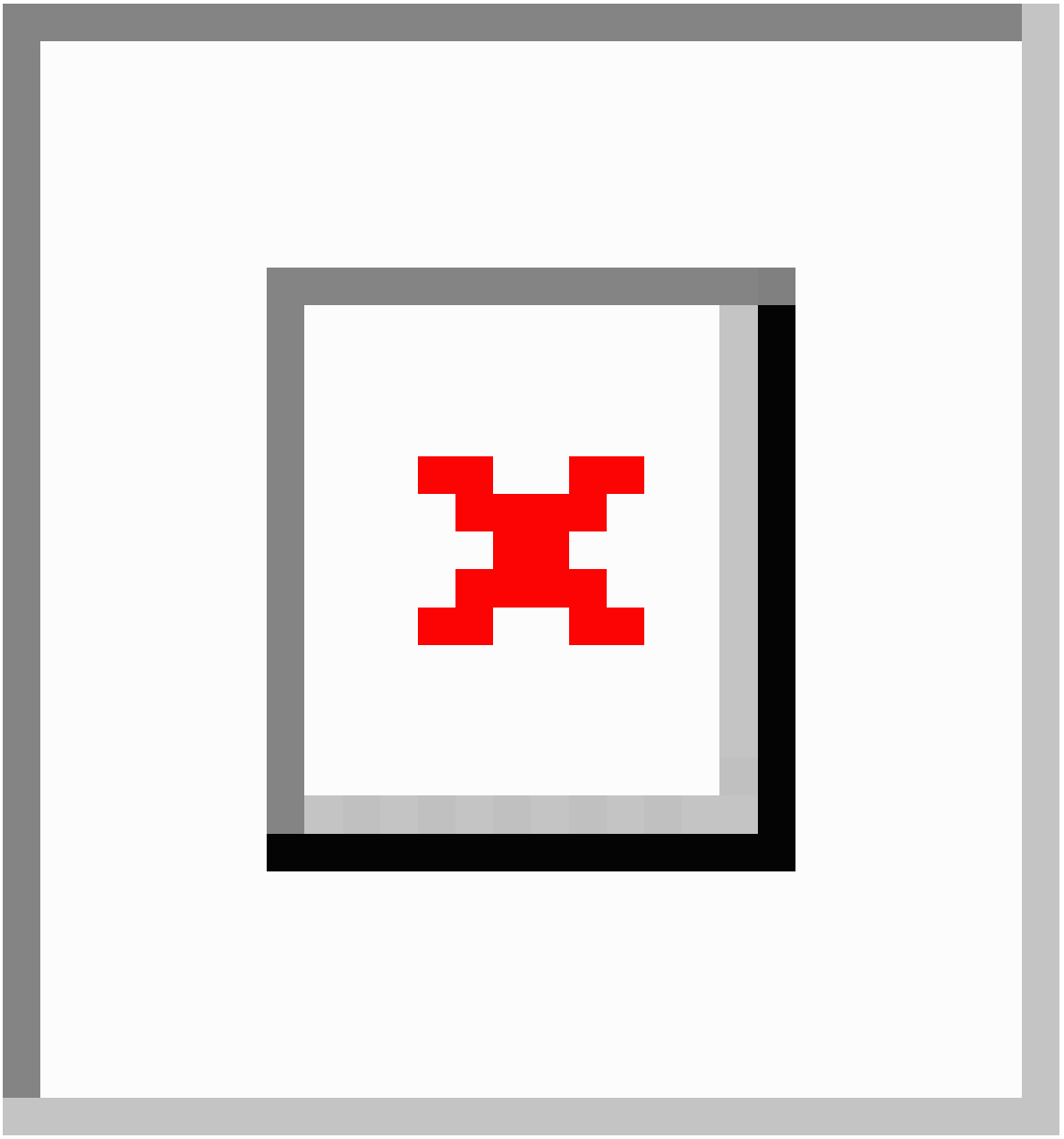
  Ne modifiez pas l'algorithme globalement; vous pouvez profiter de l'algorithme adaptatif pour la liaison homologue VSS.

- Contrairement aux grappes de matériel ASA, les grappes Firepower 4100/9300 prennent en charge la convergence progressive LACP. Ainsi, pour la plateforme, vous pouvez laisser la convergence progressive LACP activée sur les commutateurs Cisco Nexus connectés.
- Lorsque vous voyez le regroupement lent d'un EtherChannel étendu sur le commutateur, vous pouvez activer un débit LACP rapide pour une interface individuelle sur le commutateur. Le débit du protocole LACP de FXOS EtherChannels est rapide par défaut. Notez que certains commutateurs, comme la série Nexus, ne prennent pas en charge le débit LACP rapide lors des mises à niveau logicielles en service (ISSU). Nous ne recommandons donc pas l'utilisation des ISSU avec la mise en grappe.

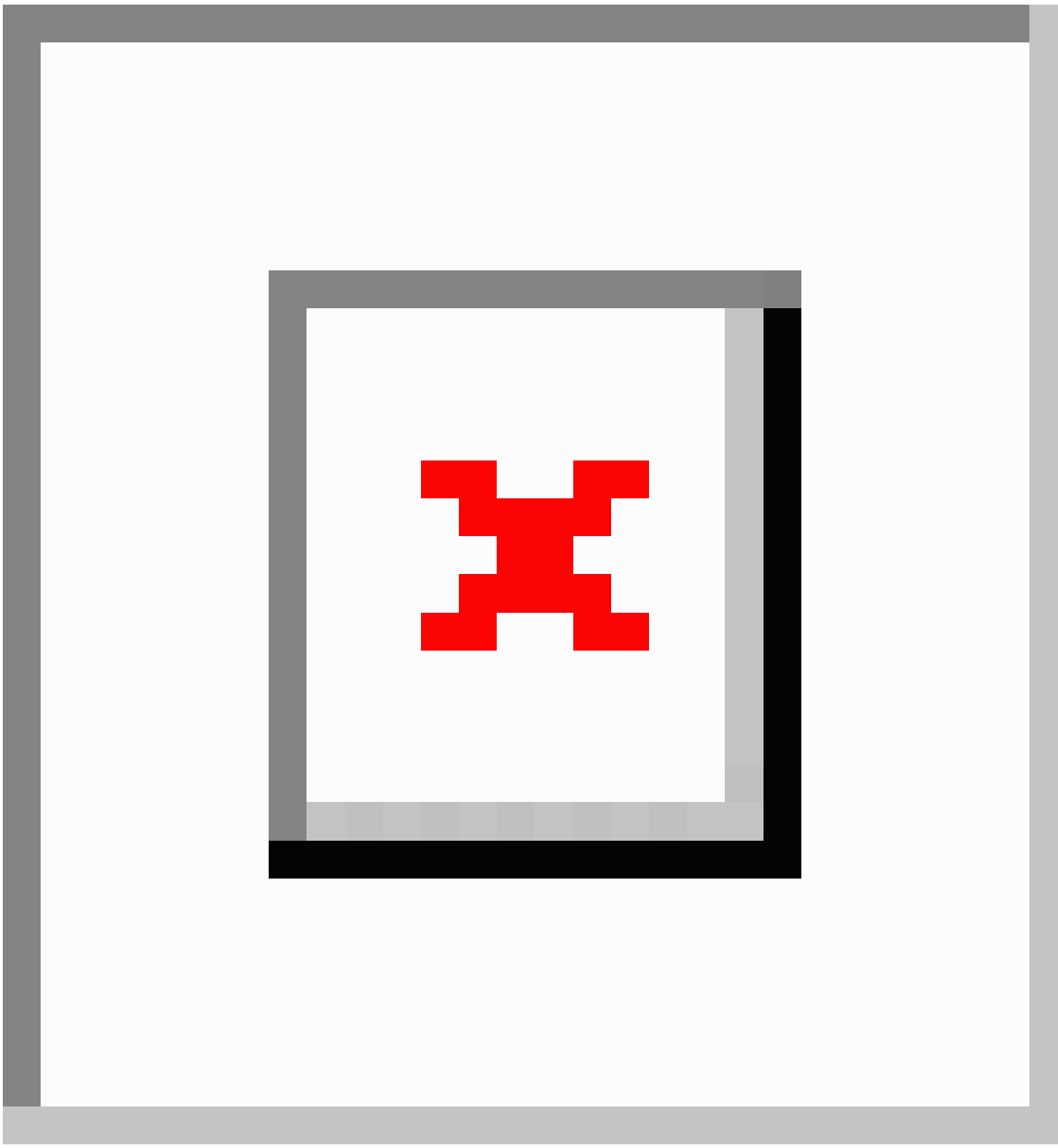
EtherChannels pour la mise en grappe

- Dans les versions du logiciel Cisco IOS Catalyst 3750-X antérieures à la15.1(1)S2, l'unité de grappe ne prenait pas en charge la connexion d'un EtherChannel à une pile de commutateurs. Avec les paramètres par défaut du commutateur, si l'EtherChannel de l'unité de grappe est connecté de manière croisée et si le commutateur de l'unité de contrôle est hors tension, l'EtherChannel connecté au commutateur restant ne s'activera pas. Pour améliorer la compatibilité, définissez la commande **stack-mac persistent timer** sur une valeur suffisamment grande pour prendre en compte le temps de rechargement; par exemple, 8 minutes ou 0 pour indéfini. Vous pouvez également effectuer une mise à niveau vers une version plus stable du logiciel du commutateur, comme par exemple 15.1(1)S2.
- Configuration des EtherChannels étendus vs. locaux au périphérique : veillez à configurer le commutateur de manière appropriée pour les EtherChannels étendus par rapport aux EtherChannels locaux au périphérique.
  - EtherChannels étendus : pour les EtherChannels *étendus* des unités de grappe, qui s'étendent sur tous les membres de la grappe, les interfaces sont combinées en un seul EtherChannel sur le

commutateur. Vérifiez que chaque interface se trouve dans le même groupe de canaux sur le commutateur.



- EtherChannels locaux au périphérique : pour les EtherChannels *locaux au périphérique* de grappe, y compris tous les EtherChannels configurés pour la liaison de commande de la grappe, veillez à configurer des EtherChannels isolés sur le commutateur; ne combinez pas plusieurs EtherChannels d'unités de grappe en un seul EtherChannel sur le commutateur.



Mise en grappe inter-sites

Consultez les consignes suivantes concernant la mise en grappe inter-sites :

- La latence de la liaison de commande de grappe doit être inférieure à 20 ms temps aller-retour (RTT).
- La liaison de commande de grappe doit être fiable, sans paquets dans le désordre ou abandonnés; par exemple, vous devez utiliser un lien dédié.
- Ne configurez pas le rééquilibrage de connexion; il ne faut pas que les connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

- L'ASA ne chiffre pas le trafic de données transféré sur la liaison de commande de grappe, car il s'agit d'un lien dédié, même lorsqu'il est utilisé sur une interconnexion de centre de données (DCI). Si vous utilisez la virtualisation du transport par superposition (OTV), ou étendez la liaison de commande de grappe en dehors du domaine administratif local, vous pouvez configurer le chiffrement sur vos routeurs de frontière, comme 802.1AE MacSec sur OTV.
- La mise en œuvre de la grappe ne fait pas de différence entre les membres de plusieurs sites pour les connexions entrantes; par conséquent, les rôles de connexion pour une connexion donnée peuvent s'étendre sur plusieurs sites. Il s'agit du comportement attendu. Toutefois, si vous activez la localisation de directeur, le rôle de directeur local est toujours choisi sur le même site que le propriétaire de la connexion (selon l'ID du site). En outre, le directeur local choisit un nouveau propriétaire sur le même site si le propriétaire d'origine tombe en panne (Remarque : si le trafic est dissymétrique entre les sites et qu'il y a un trafic continu en provenance du site distant après la défaillance du propriétaire d'origine, alors un nœud du site distant site peut devenir le nouveau propriétaire s'il reçoit un paquet de données pendant la fenêtre de réhébergement.).
- Pour la localisation du directeur, les types de trafic suivants ne prennent pas en charge la localisation : le trafic NAT ou PAT; trafic inspecté par SCTP; requête du propriétaire de la fragmentation.
- Dans un déploiement Nord-Sud avec des flux UDP persistants, des boucles de routage peuvent se produire si les nœuds du site propriétaire initial du flux tombent en panne, puis reviennent en ligne, ce qui entraîne une redirection du flux vers le site d'origine. Si le nouveau propriétaire, sur l'autre site, ne dispose pas d'une route vers la destination, il redirigera le flux vers Internet, créant ainsi une boucle. Dans ce cas, utilisez la commande **clear conn** sur le nouveau propriétaire pour forcer la réinitialisation du flux.
- Pour le mode transparent, si la grappe est placée entre une paire de routeurs internes et externes (AKA insertion nord-sud), vous devez vous assurer que les deux routeurs internes partagent une adresse MAC et que les deux routeurs externes partagent une adresse MAC. Lorsqu'un membre de la grappe sur le site 1 transfère une connexion à un membre du site 2, l'adresse MAC de destination est conservée. Le paquet n'atteindra le routeur du site 2 que si l'adresse MAC est la même que celle du routeur du site 1.
- Pour le mode transparent, si la grappe est placée entre les réseaux de données et le routeur de passerelle de chaque site pour le pare-feu entre les réseaux internes (AKA insertion est-ouest), chaque routeur de passerelle doit utiliser un protocole FHRP (First Hop Redundancy Protocol) comme HSRP pour fournir des destinations d'adresses IP et MAC virtuelles identiques sur chaque site. Les VLAN de données sont étendus à l'ensemble des sites à l'aide de la virtualisation du transport par superposition (OTV), ou d'un outil similaire. Vous devez créer des filtres pour empêcher le trafic destiné au routeur de la passerelle local d'être envoyé à l'autre site sur DCI. Si le routeur de la passerelle devient inaccessible sur un site, vous devez supprimer les filtres pour que le trafic puisse atteindre la passerelle de l'autre site.
- Pour le mode transparent, si la grappe est connectée à un routeur HSRP, vous devez ajouter l'adresse MAC HSRP du routeur en tant qu'entrée de tableau d'adresses MAC statiques sur ASA (voir Ajouter une adresse MAC statique pour les groupes de ponts, à la page 839). Lorsque des routeurs adjacents utilisent HSRP, le trafic destiné à l'adresse IP HSRP sera envoyé à l'adresse MAC HSRP, mais le trafic retour proviendra de l'adresse MAC de l'interface d'un routeur particulier dans la paire HSRP. Par conséquent, le tableau d'adresses MAC ASA n'est généralement mis à jour que lorsque l'entrée du tableau ARP ASA pour l'adresse IP HSRP expire et que l'ASA envoie une demande ARP et reçoit une réponse. Étant donné que les entrées du tableau ARP de l'ASA expirent après 14 400 secondes par défaut, mais que l'entrée du tableau d'adresses MAC expire après 300 secondes par défaut, une entrée d'adresse MAC statique est requise pour éviter les pertes de trafic liées à l'expiration du tableau.
- Pour le mode routé à l'aide de l'EtherChannel étendu, configurez les adresses MAC propres au site. Étendre les VLAN de données à tous les sites à l'aide d'OTV ou d'un outil similaire. Vous devez créer des filtres pour empêcher le trafic destiné à l'adresse MAC globale d'être envoyé à l'autre site par DCI.

Si la grappe devient inaccessible sur un site, vous devez supprimer les filtres pour que le trafic puisse atteindre les nœuds de la grappe de l'autre site. Le routage dynamique n'est pas pris en charge lorsqu'une grappe inter-sites sert de routeur de premier saut pour un segment étendu.

Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'Châssis Firepower 4100/9300 ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise, ou StackWise Virtual), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.
- lors de l'ajout d'une unité à une grappe existante ou lors du rechargement d'une unité, il se produira une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent suspendre les connexions; Par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Si vous utilisez un serveur Windows 2003 connecté à une interface EtherChannel étendue, lorsque le port du serveur syslog est en panne et que le serveur ne limite pas les messages d'erreur ICMP, un grand nombre de messages ICMP sont renvoyés à la grappe. Ces messages peuvent faire en sorte que certaines unités de la grappe connaissent un niveau élevé de CPU, ce qui peut affecter les performances. Nous vous recommandons de limiter les messages d'erreur ICMP.
- Nous vous recommandons de connecter les EtherChannels à un VSS, à un vPC, à StackWise ou à StackWise Virtual pour la redondance.
- Dans un châssis, vous ne pouvez pas mettre en grappe certains modules de sécurité et exécuter d'autres modules de sécurité en mode autonome; vous devez inclure tous les modules de sécurité dans la grappe.

Valeurs par défaut

- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- Le rééquilibrage de la connexion est désactivé par défaut. Si vous activez le rééquilibrage de la connexion, l'intervalle par défaut entre les échanges d'informations de chargement est de 5 secondes.
- La fonction de jonction automatique de la grappe pour une liaison de commande de grappe défaillante est définie pour permettre un nombre illimité de tentatives toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante est définie à 3 tentatives toutes les 5 minutes, avec un intervalle croissant défini à 2.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe sur le Châssis Firepower 4100/9300

Vous pouvez facilement déployer la grappe à partir du superviseur Châssis Firepower 4100/9300 . Toute la configuration initiale est générée automatiquement pour chaque unité. Cette section décrit la configuration du démarrage par défaut et la personnalisation facultative que vous pouvez effectuer sur l'ASA. Cette section

décrit également comment gérer les membres de la grappe à partir de l'ASA. Vous pouvez également gérer l'appartenance à la grappe à partir du Châssis Firepower 4100/9300 . Pour obtenir de plus amples renseignements, consultez la documentation du Châssis Firepower 4100/9300 .

Procédure

Étape 1 FXOS : Ajouter une grappe ASA, à la page 468
Étape 2 ASA : Modifier le mode de pare-feu et le mode de contexte, à la page 476
Étape 3 ASA : Configurer les interfaces de données, à la page 476
Étape 4 ASA : Personnaliser la configuration de la grappe, à la page 479
Étape 5 ASA : Gérer les membres de la grappe, à la page 496

FXOS : Ajouter une grappe ASA

Vous pouvez ajouter un seul châssis Firepower 9300 en tant que grappe intra-châssis ou ajouter plusieurs châssis pour la mise en grappe inter-châssis. Pour la mise en grappe inter-châssis, vous devez configurer chaque châssis séparément. Ajoutez la grappe sur un châssis; vous pouvez ensuite copier la configuration de démarrage du premier châssis sur le châssis suivant pour faciliter le déploiement,

Créer une grappe ASA

Définissez la portée sur la version de l'image.

Vous pouvez facilement déployer la grappe à partir du superviseur Châssis Firepower 4100/9300 . Toute la configuration initiale est générée automatiquement pour chaque unité.

Pour la mise en grappe sur plusieurs châssis, vous devez configurer chaque châssis séparément. Déployer la grappe sur un châssis; vous pouvez ensuite copier la configuration de démarrage du premier châssis au châssis suivant pour faciliter le déploiement.

Dans un châssis Firepower 9300, vous devez activer la mise en grappe pour les 3 logements de module , même si aucun module n'est installé. Si vous ne configurez pas les 3 modules, la grappe ne s'affichera pas.

Pour le mode à contextes multiples, vous devez d'abord déployer le périphérique logique, puis activer le mode à contextes multiples dans l'application ASA.

Lorsque vous déployez une grappe, le superviseur Châssis Firepower 4100/9300 configure chaque application ASA avec la configuration de démarrage suivante. Vous pouvez modifier ultérieurement, si vous le souhaitez, des parties de la configuration de démarrage à partir de l'ASA (en **gras**).

```
interface Port-channel48
   description Clustering Interface
cluster group <service_type_name>
   key <secret>
   local-unit unit-<chassis#-module#>
   site-id <number>
   cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
   priority <auto>
   health-check holdtime 3
   health-check data-interface auto-rejoin 3 5 2
   health-check cluster-interface auto-rejoin unlimited 5 1
```

```
   enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
   management-only individual
   nameif management
   security-level 0
   ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
   no shutdown

http server enable
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1
```



Remarque Le nom **local-unit** ne peut être modifié que si vous désactivez la mise en grappe.

Avant de commencer

- Téléchargez l'image de l'application que vous voulez utiliser pour l'appareil logique à partir de Cisco.com, puis téléchargez cette image sur le serveur de l'application Châssis Firepower 4100/9300 .
- Recueillez les informations suivantes :
  - ID de l'interface de gestion, adresses IP et masque de réseau
  - Adresse IP de la passerelle

Procédure

Étape 1 Configurer les interfaces.

a) Ajoutez au moins une interface de type de données ou un EtherChannel (également appelé canal de port) avant de déployer la grappe. Reportez-vous aux sections Ajouter un canal EtherChannel (canal de port), à la page 207 ou Configurer une interface physique, à la page 206.

Pour la mise en grappe sur plusieurs châssis, toutes les interfaces de données doivent être des EtherChannels étendus avec au moins une interface membre. Ajoutez les mêmes EtherChannels sur chaque châssis. Combinez les interfaces membres de toutes les unités de la grappe en un seul EtherChannel sur le commutateur. Consultez Lignes directrices et limites de la mise en grappe, à la page 462 pour obtenir des renseignements sur les EtherChannels.

b) Ajoutez une interface de type de gestion ou un EtherChannel. Reportez-vous aux sections Ajouter un canal EtherChannel (canal de port), à la page 207 ou Configurer une interface physique, à la page 206.

L'interface de gestion est requise. Notez que cette interface de gestion n'est pas la même que l'interface de gestion du châssis qui est utilisée uniquement pour la gestion de ce dernier (dans FXOS, vous pouvez voir l'interface de gestion du châssis affichée comme MGMT, management0, ou d'autres noms similaires).

Pour la mise en grappe sur plusieurs châssis, ajoutez la même interface de gestion sur chaque châssis.

c) Pour la mise en grappe sur plusieurs châssis, ajoutez une interface membre à l'EtherChannel de la liaison de commande de grappe (par défaut, le canal de port 48). Consultez Ajouter un canal EtherChannel (canal de port), à la page 207.

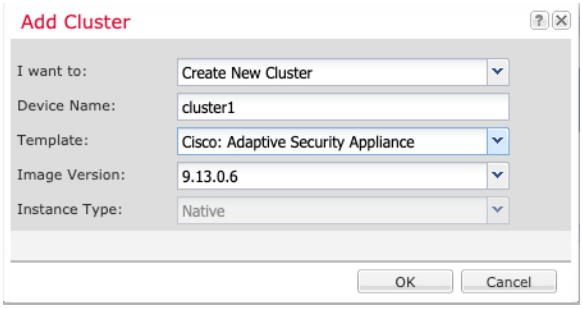
N'ajoutez pas d'interface membre pour une grappe isolée aux modules de sécurité dans un châssis Firepower 9300. Si vous ajoutez un membre, le châssis suppose que cette grappe utilisera plusieurs châssis et vous permettra uniquement d'utiliser des EtherChannels étendus, par exemple.

Sous l'onglet **Interfaces**, l'interface de type de grappe du canal de port 48 affiche l' **état de l'opération** comme **ayant échoué** si elle n'inclut aucune interface membre. Pour une grappe isolée de modules de sécurité dans un châssis Firepower 9300, cet EtherChannel ne nécessite aucune interface membre et vous pouvez ignorer cet état opérationnel.

Ajoutez les mêmes interfaces membre sur chaque châssis. La liaison de commande de grappe est un EtherChannel local au périphérique sur chaque châssis. Utilisez des EtherChannels distincts sur le commutateur pour chaque périphérique. Consultez Lignes directrices et limites de la mise en grappe, à la page 462 pour obtenir des renseignements sur les EtherChannels.

Étape 2 Choisissez **Logical Devices** (périphériques logiques).

Étape 3 Cliquez sur **Add** > **Cluster**, (Ajouter > Grappe > Ajouter un périphérique) et définissez les paramètres suivants :



a) Choisir **Je veux :** > **Créer une nouvelle grappe**
b) Indiquez un nom de périphérique (**Device Name**).

Ce nom est utilisé en interne par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de périphérique utilisé dans la configuration de l'application.

c) pour le **Template** (modèle), choisissez **Cisco: Adaptive Security Appliance** (Cisco : Appareil de sécurité adaptable).
d) Choisissez la version de l'image (**Image Version**).
e) Pour le **type d'instance**, seul le type **natif** est pris en charge.
f) Cliquez sur **OK**.

Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du périphérique).

Étape 4 Choisissez les interfaces que vous souhaitez affecter à cette grappe.

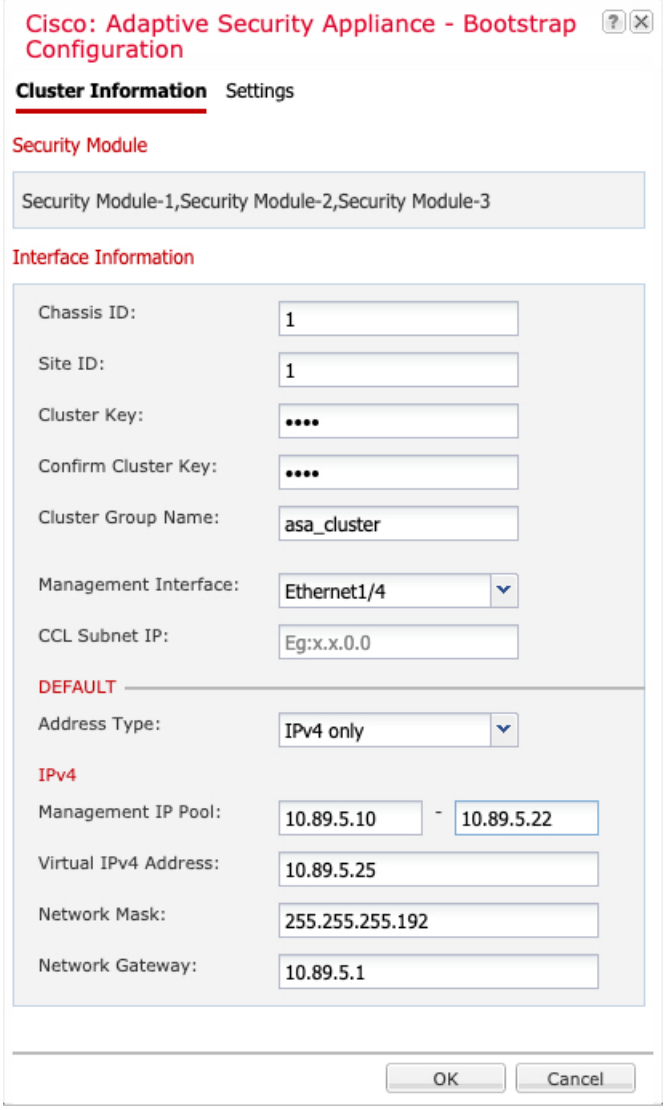
Toutes les interfaces valides sont affectées par défaut. Si vous avez défini plusieurs interfaces de type grappe, désélectionnez toutes les interfaces sauf une.

Étape 5 Cliquez sur l'icône de périphérique au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un

fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 6 Dans la page des informations de la grappe(**Cluster Information**), procédez comme suit :



a) Pour la mise en grappe sur plusieurs châssis, dans le champ **Chassis ID**, saisissez un ID de châssis. Chaque châssis de la grappe doit utiliser un ID unique.

   Ce champ ne s'affiche que si vous avez ajouté une interface membre au canal de port 48 de la liaison de commande de grappe.

b) Pour la mise en grappe inter-sites, dans le champ **Site ID**, saisissez l'ID de site pour ce châssis entre 1 et 8.

c) Dans le champ **Cluster Key** (clé de la grappe), configurez une clé d'authentification pour le trafic de contrôle sur la liaison de commande de la grappe.

Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères. Le code secret partagé est utilisé pour générer la clé de chiffrement. Cette option n'influe pas sur le trafic datapath, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair.

d) Définissez le **nom du groupe de grappes**, qui est le nom du groupe de grappes dans la configuration de périphérique logique.

Le nom doit être une chaîne ASCII comptant de 1 à 38 caractères.

Important À partir de la version 2.4.1, les espaces dans le nom de groupe de la grappe seront considérés comme des caractères spéciaux et peuvent entraîner une erreur lors du déploiement des périphériques logiques. Pour éviter ce problème, vous devez renommer le nom du groupe de grappe sans espace.

e) Choisissez l'interface de gestion (**Management Interface**).

Cette interface est utilisée pour gérer le périphérique logique. Cette interface est distincte du port de gestion du châssis.

f) Choisissez l'interface de gestion **Type d'adresse**.

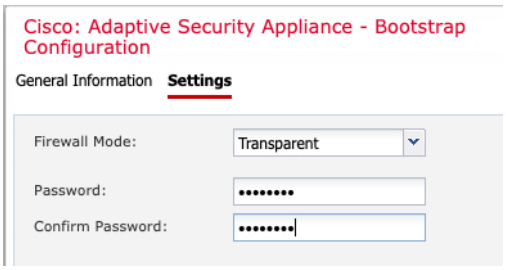
Ces informations sont utilisées pour configurer une interface de gestion dans la configuration ASA. Définissez les informations suivantes :

- **Ensemble d'adresses IP de gestion** : configurez un ensemble d'adresses IP locales, dont une sera affectée à chaque unité de grappe pour l'interface, en saisissant les adresses de début et de fin séparées par un tiret.

  Incluez au moins autant d'adresses qu'il y a d'unités dans la grappe. Notez que pour le périphérique Firepower 9300, vous devez inclure 3 adresses par châssis, même si tous les logements de module ne sont pas remplis. Si vous prévoyez d'étendre la grappe, incluez des adresses supplémentaires. L'adresse IP virtuelle (appelée adresse IP de la grappe principale) qui appartient à l'unité de contrôle actuelle ne fait *pas* partie de cet ensemble; Assurez-vous de réserver une adresse IP sur le même réseau pour l'adresse IP de la grappe principale. Vous pouvez utiliser des adresses IPv4 et/ou IPv6.

- **Masque de réseau** ou **Longueur du préfixe**
- **Passerelle réseau**
- **Virtual IP address** (adresse IP virtuelle) : définit l'adresse IP de gestion de l'unité de contrôle actuelle. Cette adresse IP doit être sur le même réseau que les adresses de l'ensemble d'adresses de la grappe, mais ne doit pas faire partie de ce dernier.

Étape 7 Dans la page **Settings** (paramètres), procédez comme suit.



a) Dans la liste déroulante **Mode de pare-feu**, choisissez **Transparent** ou **Routé**.

En mode routage, l'Firewall Threat Defense est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

b) Saisissez et confirmez un mot de **passe** pour l'utilisateur admin et pour le mot de passe d'activation.

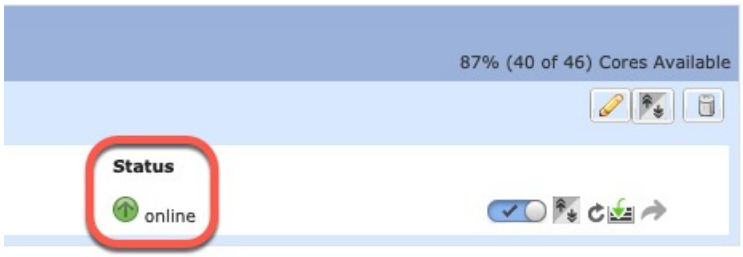
L'utilisateur admin ASA préconfiguré est utile pour la récupération du mot de passe; si vous avez un accès FXOS, vous pouvez réinitialiser le mot de passe de l'utilisateur admin en cas d'oubli.

Étape 8 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 9 Cliquez sur **Save** (Enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez l'état du nouveau périphérique logique dans la page **Logical Devices**. Lorsque le périphérique logique affiche son **état** comme **en ligne**, vous pouvez ajouter le châssis restant de la grappe ou, pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, commencer à configurer la grappe dans l'application. Vous pourriez voir l'état « Security module not responding » (module de sécurité ne répond pas) dans le cadre du processus; cet état est normal et temporaire.





Étape 10 Pour la mise en grappe sur plusieurs châssis, ajoutez le châssis suivant à la grappe :

a) Sur le premier châssis de Firewall Chassis Manager, cliquez sur l'icône **Show Configuration** (afficher la configuration) dans le coin supérieur droit; copiez la configuration de grappe affichée.
b) Connectez-vous à Firewall Chassis Manager sur le châssis suivant et ajoutez un périphérique logique en fonction de cette procédure.
c) Choisissez **Je veux : > Rejoindre une grappe existante**.
d) - **OK**.
e) Dans la zone **Copy Cluster Details** (copier les détails de la grappe), collez la configuration de la grappe du premier châssis, puis cliquez sur **OK**.
f) Cliquez sur l'icône de périphérique au centre de l'écran. Les informations sur la grappe sont pour la plupart préremplies, mais vous devez modifier les paramètres suivants :

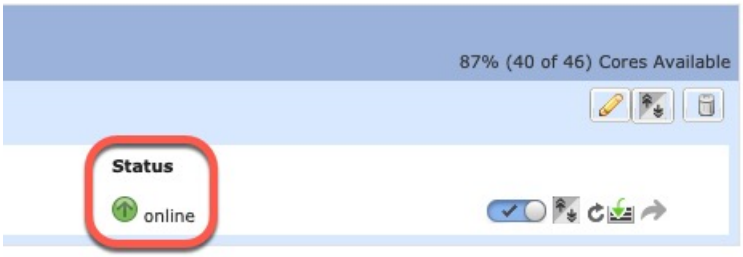
- **Chassis ID** : saisissez un ID de châssis unique.
- **Site ID** : saisissez l'ID correct du site.
- **Cluster Key**(clé de grappe) : (non préremplie) Saisissez la même clé de grappe.

Cliquez sur **OK**.

g) Cliquez sur **Save** (Enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez la page **Périphériques logiques** de chaque membre de la grappe pour connaître l'état du nouveau périphérique logique. Lorsque le périphérique logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la grappe dans l'application. Vous pourriez voir l'état « Security module not responding » (module de sécurité ne répond pas) dans le cadre du processus; cet état est normal et temporaire.





Étape 11 Connectez-vous à l'unité de contrôle ASA pour personnaliser votre configuration de mise en grappe.

Ajouter d'autres membres à la grappe

Ajoutez ou remplacez le membre de la grappe ASA.

Remarque Cette procédure s'applique uniquement à l'ajout ou au remplacement d'un *châssis*; si vous ajoutez ou remplacez un module sur un Firepower 9300 pour lequel la mise en grappe est déjà activée, le module sera ajouté automatiquement.

Avant de commencer

- Assurez-vous que votre grappe existante dispose d'un nombre suffisant d'adresses IP dans l'ensemble d'adresses IP de gestion pour ce nouveau membre. Sinon, vous devez modifier la configuration de

démarrage de grappe existante sur chaque châssis avant d'ajouter ce nouveau membre. Cette modification entraîne le redémarrage du périphérique logique.

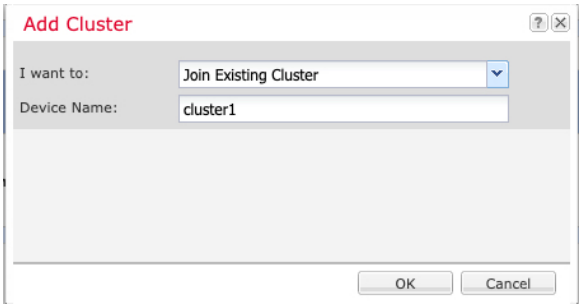
- La configuration de l'interface doit être la même sur le nouveau châssis. Vous pouvez exporter et importer la configuration du châssis FXOS pour faciliter ce processus.
- Pour le mode de contexte multiple, activez le mode de contexte multiple dans l'application ASA sur le premier membre de grappe; les membres de la grappe héritent automatiquement de la configuration en mode de contexte multiple.

Procédure

Étape 1 Sur une grappe Firewall Chassis Manager existante, choisissez **Logical Devices** (Périphériques logiques) pour ouvrir la page **Logical Devices** (Périphériques logiques).

Étape 2 Cliquez sur l'Icône afficher configuration () en haut à droite; copiez la configuration de la grappe affichée.

Étape 3 Connectez-vous à Firewall Chassis Manager sur le nouveau châssis et cliquez sur **Add** > **Cluster** (Ajouter > Grappe > Ajouter un périphérique > Ajouter un périphérique).



Étape 4 Choisissez **I want to: (Je veux :)** > **Join Existing Cluster (Rejoindre une grappe existante)**

Étape 5 Pour **Device Name** : indiquez un nom pour le périphérique.

Étape 6 cliquez sur **OK**.

Étape 7 Dans la zone **Copy Cluster Details** (copier les détails de la grappe), collez la configuration de la grappe du premier châssis, puis cliquez sur **OK**.

Étape 8 Cliquez sur l'icône de périphérique au centre de l'écran. Les informations sur la grappe sont pour la plupart préremplies, mais vous devez modifier les paramètres suivants :

- **Chassis ID** : saisissez un ID de châssis unique.
- **Site ID** : saisissez l'ID correct du site.
- **Cluster Key**(clé de grappe) : (non préremplie) Saisissez la même clé de grappe.

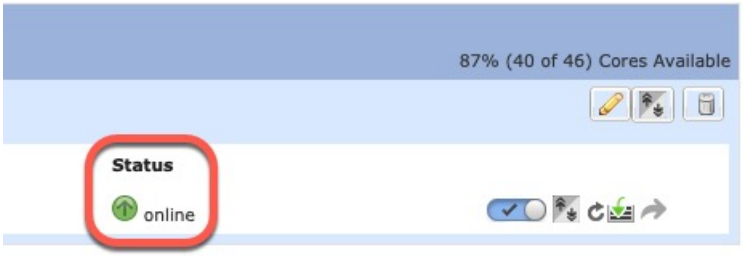
Cliquez sur **OK**.

Étape 9 Cliquez sur **Save** (Enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez la page **Périphériques logiques** de chaque membre de la grappe pour connaître l'état du nouveau périphérique logique. Lorsque le périphérique logique indique que son état (**Status**) est en ligne (**online**), vous pouvez

commencer à configurer la grappe dans l'application. Vous pourriez voir l'état « Security module not responding » (module de sécurité ne répond pas) dans le cadre du processus; cet état est normal et temporaire.





ASA : Modifier le mode de pare-feu et le mode de contexte

Par défaut, le châssis FXOS déploie une grappe en mode de pare-feu routé et en mode de contexte unique.

- Changer le mode de pare-feu : pour changer le mode après le déploiement, changez le mode sur l'unité de contrôle; le mode est automatiquement modifié sur toutes les unités de données pour qu'elles correspondent. Consultez Définir le mode du pare-feu (mode unique), à la page 231. En mode de contexte multiple, vous définissez le mode de pare-feu par contexte. Consultez Configurer un contexte de sécurité, à la page 276.Consultez le
- Passer en mode de contexte multiple : pour passer en mode de contexte multiple après le déploiement, modifiez le mode sur l'unité de contrôle; le mode est automatiquement modifié sur toutes les unités de données pour qu'elles correspondent. Voir Activer le mode de contexte multiple, à la page 270.

ASA : Configurer les interfaces de données

Cette procédure configure les paramètres de base pour chaque interface de données que vous avez affectée à la grappe lorsque vous l'avez déployée dans FXOS. Pour la mise en grappe sur plusieurs châssis, les interfaces de données sont toujours des interfaces EtherChannel étendus.

Remarque L'interface de gestion a été préconfigurée lorsque vous avez déployé la grappe. Vous pouvez également modifier les paramètres de l'interface de gestion dans l'ASA, mais cette procédure se concentre sur les interfaces de données. L'interface de gestion est une interface individuelle spéciale, par opposition à une interface étendue. Consultez Interface de gestion, à la page 456 pour de plus amples renseignements.

Avant de commencer

- Pour le mode de contexte multiple, commencez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système dans le volet Configuration > Device List (Liste des périphériques) et double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.
- Pour le mode transparent, configurez le groupe de ponts. Consultez Configurer la BVI (Bridge Virtual Interface), à la page 702.
- Lorsque vous utilisez des EtherChannels étendus pour une grappe avec plusieurs châssis, l'interface du canal de port ne s'affiche pas tant que la mise en grappe n'est pas complètement activée. Cette exigence empêche le trafic d'être transféré vers un nœud qui n'est pas un nœud actif dans la grappe.

Procédure

Étape 1 Selon votre mode de contexte :

- Pour le mode unique, choisissez le volet **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces**.
- Pour le mode multiple dans l'espace d'exécution du système, choisissez le volet **Configuration > Context Management (Gestion des contextes) > Interfaces** .

Étape 2 Sélectionnez l'interface, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche.

Étape 3 Définissez les paramètres suivants :

- (Pour les EtherChannels) **MIO Port-canal ID** (ID de canal de port MIO) : saisissez le même ID que celui utilisé dans FXOS.
- **Enable Interface** (Activer l'interface) (coché par défaut)

Les autres champs de cet écran sont décrits plus loin au cours de cette procédure.

Étape 4 Pour configurer l'adresse MAC et les paramètres facultatifs, cliquez sur l'onglet **Advanced** (Avancé).

- Dans la zone **MAC Address Cloning** (Clonage de l'adresse MAC), définissez une adresse MAC globale manuelle pour l'EtherChannel. Ne définissez pas l'adresse MAC en veille; elle est ignorée. Vous devez configurer une adresse MAC pour un EtherChannel étendu afin d'éviter d'éventuels problèmes de connectivité au réseau. Dans le cas d'une adresse MAC configurée manuellement, l'adresse MAC reste celle de l'unité de contrôle actuelle. Si vous ne configurez pas d'adresse MAC, si l'unité de contrôle change, la nouvelle unité de contrôle utilisera une nouvelle adresse MAC pour l'interface, ce qui peut provoquer une panne temporaire du réseau.

  En mode de contexte multiple, si vous partagez une interface entre les contextes, vous devez plutôt activer la génération automatique des adresses MAC pour ne pas avoir à définir l'adresse MAC manuellement. Notez que vous devez configurer manuellement l'adresse MAC à l'aide de cette commande pour les interfaces *non partagées*.
- Dans la zone **ASA Cluster** (Grappe ASA), pour la mise en grappe inter-sites, définissez **Site specific MAC Addresses (Adresses MAC spécifiques au site)** et pour le mode routé, les adresses IP d'un site en cliquant sur **Add** (Ajouter) et en spécifiant une adresse MAC et une adresse IP pour l'ID de site (1 à

8). Répétez l'opération pour un maximum de 8 sites. Les adresses IP spécifiques au site doivent se trouver sur le même sous-réseau que l'adresse IP globale. L'adresse MAC spécifique au site et l'adresse IP utilisées par une unité dépendent de l'ID de site que vous spécifiez dans la configuration de démarrage de chaque unité.

Étape 5 (Facultatif) Configurez les sous-interfaces VLAN sur cet EtherChannel. Le reste de cette procédure s'applique aux sous-interfaces.

Étape 6 (Mode de contexte multiple) Avant de terminer cette procédure, vous devez attribuer des interfaces aux contextes.

a) Cliquez sur **OK** pour accepter vos modifications.
b) Allouez les interfaces.
c) Passez au contexte que vous souhaitez configurer : dans le volet **Device List** (Liste des périphériques), double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.
d) Choisissez le volet **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces**, sélectionnez l'interface de canal de port que vous souhaitez personnaliser, puis cliquez sur **Edit**(Modifier).

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche.

Étape 7 Cliquez sur l'onglet **General** (Général).

Étape 8 (Mode transparent) Dans la liste déroulante **Bridge Group** (Groupe de ponts), choisissez le groupe de ponts auquel vous souhaitez affecter cette interface.

Étape 9 Dans le champ **Interface Name** (Nom d'interface), saisissez un nom renfermant au maximum 48 caractères.

Étape 10 Dans le champ **Security level** (Niveau de sécurité), saisissez un niveau compris entre 0 (le plus bas) et 100 (le plus élevé).

Étape 11 (Mode routé) Pour une adresse IPv4, cliquez sur le bouton radio **Use Static IP** (Utiliser l'adresse IP statique) et saisissez l'adresse IP et le masque. Les protocoles DHCP et PPPoE ne sont pas pris en charge. Pour les connexions point à point, vous pouvez spécifier un filtre d'adresse locale de 31 bits (255.255.255.254). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion. Pour le mode transparent, vous configurez l'adresse IP de l'interface de groupe de ponts, et non de l'interface EtherChannel.

Étape 12 (Mode routé) Pour configurer une adresse IPv6, cliquez sur l'onglet **IPv6**.

Pour le mode transparent, vous configurez l'adresse IP de l'interface de groupe de ponts, et non de l'interface EtherChannel.

a) Cochez la case **Enable IPv6** (Activer IPv6).
b) Dans la zone **Interface IPv6 Addresses** (Adresses IPv6 de l'interface), cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add IPv6 Address for Interface** (ajouter une adresse IPv6 pour l'interface) s'affiche.



Remarque L'option **Enable address autoconfiguration** (Activer l'autoconfiguration de l'adresse) n'est pas prise en charge. La configuration manuelle de l'adresse Link-Local n'est pas non plus prise en charge.

c) Dans le champ **Address/Prefix Length** (Longueur d'adresse/préfixe), saisissez l'adresse IPv6 globale et la longueur du préfixe IPv6. Par exemple, 2001:DB8::BA98:0:3210/64.
d) (Facultatif) Pour utiliser l'ID d'interface EUI-64 modifié comme adresse d'hôte, cochez la case **EUI-64**. Dans ce cas, saisissez le préfixe dans le champ **Address/Prefix Length** (Longueur d'adresse/préfixe).
e) Cliquez sur **OK**.

Étape 13 Cliquez sur **OK** pour revenir à l'écran **Interfaces**.

Étape 14 Cliquez sur **Apply** (Appliquer).

ASA : Personnaliser la configuration de la grappe

Si vous souhaitez modifier les paramètres de démarrage après avoir déployé la grappe ou configuré des options supplémentaires, comme la surveillance de l'intégrité de la grappe, le délai de réplication de la connexion TCP, la mobilité des flux et d'autres optimisations, vous pouvez le faire sur l'unité de contrôle.

Configurer les paramètres de grappe ASA de base

Vous pouvez personnaliser les paramètres de grappe sur le nœud de contrôle.

Avant de commencer

- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système sur l'unité de contrôle. Si vous n'êtes pas déjà en mode de configuration système, dans le volet **Configuration** > **Device List (Liste des périphériques)**, double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.
- Le **nom de membre** de l'unité locale et plusieurs autres options ne peuvent être définis que sur le châssis FXOS, ou ils ne peuvent être modifiés que sur l'ASA si vous désactivez la mise en grappe. Ils ne sont donc pas inclus dans la procédure suivante.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**.

Étape 2 (Facultatif) Configurez les paramètres facultatifs suivants :

- **Cluster Member Limit** (Limite de membres de la grappe) : configurez le nombre maximum de membres de la grappe, entre 2 et 16. Par défaut, c'est 16. Si vous savez que votre grappe sera inférieure au maximum de 16 unités, nous vous conseillons de définir le nombre d'unités réel planifié. La définition du nombre maximum d'unités permet à la grappe de mieux gérer les ressources. Par exemple, si vous utilisez la traduction d'adresse de port (PAT), l'unité de contrôle peut ensuite allouer des blocs de ports au nombre de membres planifié sans avoir à réserver des ports pour des unités supplémentaires que vous ne comptez pas utiliser.
- **Site Periodic GARP** (GARP périodique du site) : l'ASA génère des paquets ARP gratuits (GARP) pour maintenir l'infrastructure de commutation à jour : le membre ayant la priorité la plus élevée sur chaque site génère périodiquement du trafic GARP pour les adresses MAC et IP globales. Le GARP est activé par défaut lorsque vous définissez l'ID de site pour chaque unité et l'adresse MAC et IP du site pour chaque EtherChannel étendu. Définissez l'intervalle GARP entre 1 et 1 000 000 secondes. La valeur par défaut est de 290 secondes.

  Lorsque vous utilisez des adresses MAC et IP par site, les paquets provant de la grappe utilisent une adresse MAC et une adresse IP propres au site, tandis que les paquets reçus par la grappe utilisent une adresse MAC et une adresse IP globales. Si le trafic n'est pas généré périodiquement à partir de l'adresse

MAC globale, vous pourriez rencontrer un délai d'expiration de l'adresse MAC sur vos commutateurs pour l'adresse MAC globale. Après un délai d'expiration, le trafic destiné à l'adresse MAC globale sera inondé dans l'ensemble de l'infrastructure de commutation, ce qui peut entraîner des problèmes de performance et de sécurité.

- **Enable connection rebalancing for TCP traffic across all the ASAs in the cluster** (Activer le rééquilibrage de connexion pour le trafic TCP sur tous les ASA de la grappe) : permet de rééquilibrer la connexion. Le paramètre par défaut de ce filtre est désactivé. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données. Si cette option est activée, les ASA échangent périodiquement des renseignements sur les connexions par seconde et déchargent les nouvelles connexions des appareils ayant plus de connexions par seconde vers les appareils moins chargés. Les connexions existantes ne sont jamais déplacées. De plus, comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal. La fréquence, comprise entre 1 et 360 secondes, spécifie la fréquence à laquelle les informations de chargement sont échangées. La valeur par défaut est de 5 secondes.

  Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

  Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

- **Enable cluster load monitor** (Activer le moniteur de charge de la grappe) : vous pouvez superviser la charge de trafic pour les membres de la grappe, y compris le nombre total de connexions, l'utilisation du CPU et de la mémoire, ainsi que les abandons de tampon. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur l'unité si les unités restantes peuvent gérer la charge ou de régler l'équilibrage de charges sur le commutateur externe. Cette fonction est activée par défaut. Par exemple, pour la mise en grappe inter-châssis sur le Firepower 9300 avec 3 modules de sécurité dans chaque châssis, si deux modules de sécurité d'un châssis quittent la grappe, la même quantité de trafic vers le châssis sera envoyée au module restant et risque de le submerger. Vous pouvez superviser périodiquement la charge de trafic. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur l'unité.

  Définissez les paramètres suivants :

  - **Time Interval** (Intervalle de temps) : définit le temps en secondes entre les messages de supervision, entre 10 et 360 secondes. La valeur par défaut est de 20 secondes.
  - **Number of Intervals** (Nombre d'intervalles) : définit le nombre d'intervalles pour lesquels l'ASA conserve les données, entre 1 et 60. La valeur par défaut est 30.

  Consultez **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Load-Monitoring (Supervision de la charge de la grappe)** pour afficher la charge de trafic.

- **Enable health monitoring of this device within the cluster** (Activer la surveillance de l'intégrité de ce périphérique dans la grappe) : active la fonctionnalité de vérification de l'intégrité des unités de la grappe et détermine le temps entre les messages d'état de pulsation des unités, entre 0,3 et 45 secondes; la valeur par défaut est de 3 secondes. **Remarque** : lorsque vous ajoutez de nouvelles unités à la grappe et apportez des modifications de topologie à l'ASA ou au commutateur, vous devez désactiver temporairement cette fonctionnalité jusqu'à ce que la grappe soit terminée et désactiver la supervision d'interface pour les interfaces désactivées (**Configuration** > **Device Management [Gestion des périphériques]** > **High Availability and Scalability [Haute disponibilité et évolutivité]** > **ASA Cluster [Grappe ASA]** > **Cluster Interface Health Monitoring [Surveillance de l'intégrité de l'interface de grappe]**). Vous pouvez réactiver cette fonctionnalité une fois les modifications apportées à la grappe et à la topologie terminées. Pour déterminer l'intégrité des unités, les unités de grappe ASA

envoient à d'autres unités des messages de signal de présence heartbeat sur la liaison de commande de grappe. Si une unité ne reçoit aucun message heartbeat d'une unité homologue pendant la période d'attente, l'unité homologue est considérée comme ne répondant pas ou morte.

- **Debounce Time** (Délai antirebond) : configure le délai antirebond avant que l'ASA considère une interface comme défaillante et que l'unité ne soit retirée de la grappe. Cette fonctionnalité permet une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié avant de marquer l'interface comme défaillante, et l'unité est supprimée de la grappe. Par exemple, dans le cas d'un EtherChannel qui passe d'un état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un délai de réponse plus long peut empêcher l'interface de sembler être défaillante sur une unité de la grappe juste parce qu'une autre unité de la grappe a été plus rapide à regrouper les ports. Le délai antirebond par défaut est de 500 ms, avec une plage de 300 ms à 9 secondes.
- **Replicate console output** (Répliquer la sortie de la console) : active la réplication de la console des unités de données vers l'unité de contrôle. Par défaut, cette fonction est désactivée. L'ASA peut imprimer certains messages directement sur la console pour certains événements critiques. Si vous activez la réplication de console, les unités de données envoient les messages de console à l'unité de contrôle de sorte qu'il suffit de surveiller un seul port de console pour la grappe. Ce paramètre ne fait pas partie de la configuration de démarrage; il est répliqué à partir de l'unité de contrôle dans les unités de données.
- **Enable Clustering Flow Mobility** (Activer la mobilité des flux de grappes). Consultez Configurer l'inspection LISP, à la page 486.
- **Enable Director Localization for inter-DC cluster** (Activer la localisation du directeur pour la grappe inter-DC) : pour améliorer les performances et réduire la latence d'aller-retour dans le cas de la mise en grappe inter-sites pour les centres de données, vous pouvez activer la localisation du directeur. Les nouvelles connexions sont généralement équilibrées et appartiennent aux membres de la grappe d'un site donné. Cependant, l'ASA attribue le rôle de directeur à un membre sur *n'importe quel* site. La localisation du directeur permet des rôles de directeur supplémentaires : un directeur local sur le même site que le propriétaire et un directeur global qui peut se trouver sur n'importe quel site. Le fait de garder le propriétaire et le directeur sur le même site améliore les performances. De plus, en cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site. Le directeur global est utilisé si un membre d'une grappe reçoit des paquets pour une connexion appartenant à un autre site.
- **Site Redundancy** (Redondance de site) : pour protéger les flux contre une défaillance de site, vous pouvez activer la redondance de site. Si le propriétaire de connexion de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La localisation de directeur et la redondance de site sont des fonctionnalités distinctes; vous pouvez configurer l'un ou l'autre, ou configurer les deux.
- **Enable config sync acceleration** (Activer l'accélération de la synchronisation de la configuration) : lorsqu'une unité de données a la même configuration que l'unité de contrôle, elle ignorera la synchronisation de la configuration et se joindra plus rapidement. Cette fonction est activée par défaut. Cette fonctionnalité est configurée sur chaque unité et n'est pas répliquée de l'unité de contrôle à l'unité de données.

Remarque Certaines commandes de configuration ne sont pas compatibles avec la jonction accélérée de grappes; si ces commandes sont présentes sur l'unité, même si la jonction accélérée de grappes est activée, la synchronisation de la configuration se produira toujours. Vous devez supprimer la configuration incompatible pour que la jonction accélérée de grappes fonctionne. Utilisez la commande **show cluster info unit-join-acceleration incompatible-config** pour afficher la configuration incompatible.

- **Enable parallel configuration replicate** (Activer la réplication de configuration parallèle) : permet à l'unité de contrôle de synchroniser les modifications de configuration avec les unités de données en parallèle. Sinon, la synchronisation a lieu de manière séquentielle et peut prendre plus de temps.

Étape 3 Dans la zone **Cluster Control Link** (Liaison de commande de grappe), vous pouvez configurer la MTU de la liaison de commande de grappe. Les autres options de cette zone ne peuvent pas être configurées sur l'ASA.

- **MTU** : spécifiez l'unité de transfert maximale de l'interface de liaison de commande de grappe, qui doit être supérieure d'au moins 100 octets à la MTU la plus élevée des interfaces de données. Nous vous suggérons de définir la MTU au maximum de 9 184; la valeur minimum est de 1 400 octets. De plus, nous ne conseillons pas de définir la MTU de la liaison de commande de grappe entre 2 561 et 8 362. En raison de la gestion du groupe de blocs, cette taille de MTU n'est pas optimale pour le fonctionnement du système. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe.

  Par exemple, comme la MTU maximale est de 9 184 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9 084 octets, tandis que la liaison de commande de grappe peut être définie sur 9 184 octets.

Étape 4 (Facultatif) (Firepower 9300 uniquement) **VPN Grouping Mode** (Mode de regroupement VPN). Consultez Configurer le VPN de site à site distribué, à la page 488.

Étape 5 (Facultatif) (Firepower 9300 uniquement) Dans la zone **Parallel Join of Units Per Chassis** (Jonction parallèle des unités par châssis), vous pouvez vous assurer que les modules de sécurité d'un châssis rejoignent la grappe simultanément afin que le trafic soit réparti uniformément entre les modules. Si un module se joint très avant les autres modules, il peut recevoir plus de trafic que souhaité, car les autres modules ne peuvent pas encore partager la charge.

- **Minimum Units Required to Join** (Unités minimum requises pour rejoindre) : spécifie le nombre minimum de modules dans le même châssis qui doivent être prêts avant qu'un module puisse rejoindre la grappe (entre 1 et 3). La valeur par défaut est 1, ce qui signifie qu'un module n'attendra pas que les autres modules soient prêts avant de rejoindre la grappe. Par exemple, si vous définissez la valeur à 3, chaque module attendra le délai maximum ou jusqu'à ce que les trois modules soient prêts avant de rejoindre la grappe. Les trois modules demanderont de rejoindre la grappe presque simultanément et commenceront tous à recevoir du trafic à peu près au même moment.
- **Maximum Join Delay** (Délai maximum de jonction) : spécifie le délai maximum en minutes avant qu'un module arrête d'attendre que d'autres modules soient prêts avant de rejoindre la grappe, entre 0 et 30 minutes. La valeur par défaut est 0, ce qui signifie que le module n'attendra pas que les autres modules soient prêts avant de rejoindre la grappe. Si vous définissez les unités minimum sur 1, cette valeur doit être de 0. Si vous définissez les unités minimum sur 2 ou 3, cette valeur doit être de 1 ou plus. Cette

minuterie est définie par module, mais lorsque le premier module rejoint la grappe, toutes les autres minuteries du module se terminent et les modules restants rejoignent la grappe.

Par exemple, vous définissez les unités minimum sur 3 et le délai maximum sur 5 minutes. Lorsque le module 1 apparaît, il démarre sa minuterie de 5 minutes. Le module 2 apparaît 2 minutes plus tard et démarre sa minuterie de 5 minutes. Le module 3 apparaît 1 minute plus tard. Par conséquent, tous les modules rejoindront désormais la grappe au bout de 4 minutes; ils n'attendront pas la fin de la minuterie. Si le module 3 n'apparaît jamais, le module 1 rejoindra la grappe à la fin de sa minuterie de 5 minutes et le module 2 rejoindra également la grappe, même s'il reste 2 minutes à s'écouler; il n'attendra pas la fin de sa minuterie.

Étape 6 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de surveillance de l'intégrité de l'interface et de jonction automatique

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. Vous pouvez superviser n'importe quel ID de canal de port ou ID d'interface physique unique. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Interface Health Monitoring (Surveillance de l'intégrité de l'interface de grappe)**.

Étape 2 Sélectionnez une interface dans la zone **Monitored Interfaces** (Interfaces surveillées) et cliquez sur **Add** (Ajouter) pour la déplacer vers la zone **Unmonitored Interfaces** (Interfaces non surveillées).

Les messages d'état de l'interface détectent une défaillance de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur une unité particulière, mais qu'il y a des ports actifs sous la même interface logique sur d'autres unités, l'unité est supprimée de la grappe. Si une unité ne reçoit pas de messages d'état d'interface dans le délai de rétention, le temps avant que l'ASA ne supprime un membre de la grappe dépend du type d'interface et du fait que l'unité soit un membre établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces.

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. Vous pouvez spécifier n'importe quel ID de canal de port ou ID d'interface physique unique. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA, le Châssis Firepower 4100/9300 ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise ou StackWise Virtual), vous devez désactiver le contrôle d'intégrité (**Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**) et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.

Étape 3 Cliquez sur l'onglet **Auto Rejoin** (Jonction automatique) pour personnaliser les paramètres de la jonction automatique en cas de défaillance de l'interface, du système ou de la liaison de commande de grappe. Pour chaque type, cliquez sur **Edit** (Modifier) pour définir les éléments suivants :

- **Maximum Rejoin Attempts** (Nombre maximal de tentatives de jonction) : Permet de définir le nombre de tentatives de jonction à la grappe en sélectionnant **Unlimited** (Illimité) ou une valeur comprise entre 0 et 65 535. **0** désactive la jonction automatique. La valeur par défaut est **Unlimited** (Illimité) pour l'interface de grappe et **3** pour l'interface de données et le système.
- **Rejoin Interval** (Intervalle de jonction) : permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est **5** minutes. La durée totale maximale pendant laquelle l'unité tente de rejoindre la grappe est limitée à 14400 minutes (10 jours) à compter du dernier échec.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente en définissant la variation d'intervalle entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente) ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l'interface de grappe et **2** pour l'interface de données et le système.

Cliquez sur **Restore Defaults** pour rétablir les paramètres par défaut.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer le délai de réplication TCP de la grappe

Activez le délai de réplication de la grappe pour les connexions TCP pour aider à éliminer le « travail inutile » lié aux flux de courte durée en retardant la création du flux directeur/de sauvegarde. Notez que si une unité tombe en panne avant la création du flux directeur/de sauvegarde, ces flux ne peuvent pas être récupérés. De même, si le trafic est rééquilibré vers une autre unité avant la création du flux, le flux ne peut pas être récupéré. Vous ne devez pas activer la réplication TCP pour le trafic sur lequel vous désactivez la répartition aléatoire TCP.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster Replication (Réplication de la grappe ASA)**.

Étape 2 Cliquez sur **Add** (Ajouter) et réglez les valeurs suivantes :

- **Replication delay** (Délai de réplication) : définissez les secondes entre 1 et 15.
- **HTTP** : définissez le délai pour tout le trafic HTTP. Ce paramètre est activé par défaut pendant 5 secondes.
- **Critères de source**
  - **Source** : définissez l'adresse IP source.
  - Service : (Facultatif) Définissez le port source. En général, vous définissez soit le port source, soit le port de destination, mais pas les deux.

- **Critères de destination**
  - **Source** : définissez l'adresse IP de destination.
  - **Service** : (Facultatif) Définissez le port de destination. En général, vous définissez soit le port source, soit le port de destination, mais pas les deux.

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer les fonctionnalités inter-sites

Pour la mise en grappe inter-sites, vous pouvez personnaliser votre configuration pour améliorer la redondance et la stabilité.

Configurer la mobilité des flux de grappes

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

À propos de l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux entre les sites.

À propos de LISP

La mobilité des machines virtuelles de centres de données, comme VMware VMotion, permet aux serveurs de migrer entre les centres de données tout en maintenant les connexions avec les clients. Pour prendre en charge une telle mobilité de serveur de centre de données, les routeurs doivent être en mesure de mettre à jour la route d'entrée vers le serveur lorsqu'il se déplace. L'architecture Cisco Locator/Protocole de séparation d'ID (LISP) sépare l'identité du périphérique, ou l'identifiant de terminal (EID), de son emplacement, ou localisateur de routage, dans deux espaces de numérotation différents, ce qui rend la migration du serveur transparente pour les clients. Par exemple, lorsqu'un serveur est déplacé vers un nouveau site et qu'un client envoie du trafic vers le serveur, le routeur redirige le trafic vers le nouvel emplacement.

LISP nécessite des routeurs et des serveurs dans certains rôles, tels que le routeur de tunnel de sortie (ETR) LISP, le routeur de tunnel d'entrée (ITR), les routeurs de premier saut, le résolveur de carte (MR) et le serveur de carte (MS). Lorsque le routeur du premier saut du serveur détecte que le serveur est connecté à un autre routeur, il met à jour tous les autres routeurs et les bases de données afin que l'ITR connectée au client puisse intercepter, encapsuler et envoyer le trafic vers le nouvel emplacement du serveur.

Prise en charge du LISP Cisco Secure Firewall ASA

L'ASA n'exécute pas le LISP lui-même; il peut, cependant, inspecter le trafic LISP pour détecter les changements d'emplacement, puis utiliser ces informations pour un fonctionnement de mise en grappe transparent. Sans l'intégration du LISP, lorsqu'un serveur est déplacé vers un nouveau site, le trafic est acheminé vers un membre de la grappe ASA sur le nouveau site plutôt que vers le propriétaire d'origine du flux. Le nouvel ASA transfère le trafic vers l'ASA au niveau de l'ancien site, puis l'ancien ASA doit renvoyer le trafic vers le nouveau site pour qu'il atteigne le serveur. Ce flux de trafic est sous-optimal et est connu comme « tromboning » ou « épingle à cheveux ».

Grâce à l'intégration du LISP, les membres de la grappe ASA peuvent inspecter le trafic LISP passant entre le routeur du premier saut et l'ETR ou l'ITR, puis peuvent changer le propriétaire du flux pour qu'il se trouve sur le nouveau site.

Lignes directrices LISP

- Les membres de la grappe ASA doivent se trouver entre le routeur du premier saut et l'ITR ou l'ETR du site. La grappe ASA elle-même ne peut pas être le premier routeur de saut pour un segment étendu.
- Seuls les flux entièrement distribués sont pris en charge; les flux centralisés, les flux semi-distribués ou les flux appartenant à des nœuds individuels ne sont pas transférés vers de nouveaux propriétaires. Les flux semi-distribués comprennent des applications, telles que SIP, où tous les flux enfants appartiennent au même ASA qui possède le flux parent.
- La grappe déplace uniquement les états de flux de couche 3 et 4; certaines données d'application pourraient être perdues.
- Pour les flux de courte durée ou non essentiels pour l'entreprise, le déplacement du propriétaire peut ne pas valoir la peine. Vous pouvez contrôler les types de trafic pris en charge avec cette fonctionnalité lorsque vous configurez la politique d'inspection. Vous devez limiter la mobilité de flux au trafic essentiel.

Mise en œuvre du LISP ASA

Cette fonctionnalité comprend plusieurs configurations interdépendantes (qui sont toutes décrites dans ce chapitre) :

1. (Facultatif) Limiter les EID inspectés en fonction de l'adresse IP de l'hôte ou du serveur : le routeur de premier saut pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée, vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.
2. Inspection du trafic LISP : l'ASA inspecte le trafic LISP sur le port UDP 4342 pour détecter le message EID-notify envoyé entre le premier saut du routeur et l'ITR ou l'ETR. L'ASA gère un tableau EID qui met en corrélation l'EID et l'ID de site. Par exemple, vous devez inspecter le trafic LISP avec une adresse IP source du routeur du premier saut et une adresse de destination de l'ITR ou de l'ETR. Remarque : le trafic LISP n'a pas de directeur affecté et le trafic LISP en lui-même ne participe pas au partage de l'état de la grappe.
3. Politique de service pour activer la mobilité des flux sur le trafic spécifié : vous devez activer la mobilité des flux sur le trafic critique. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques.
4. ID de sites : l'ASA utilise l'ID de site pour chaque nœud de la grappe afin de déterminer le nouveau propriétaire.
5. Configuration au niveau de la grappe pour activer la mobilité de flux : vous devez également activer la mobilité de flux au niveau de la grappe. Ce bouton bascule marche/arrêt vous permet d'activer ou de désactiver facilement la mobilité de flux pour une classe particulière de trafic ou d'applications.

Configurer l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

Avant de commencer

- Définissez l'ID de site du châssis sur le superviseur Châssis Firepower 4100/9300 .

- Le trafic LISP n'est pas inclus dans la classe de trafic d'inspection par défaut. Vous devez donc configurer une classe distincte pour le trafic LISP dans le cadre de cette procédure.

Procédure

Étape 1 (Facultatif) Configurez une carte d'inspection LISP pour limiter les EID inspectés en fonction de l'adresse IP et pour configurer la clé partagée LISP :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **LISP**.
b) Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
c) Saisissez un nom (40 caractères maximum) et une description.
d) Pour la commande **Allowed-EID access-list**, cliquez sur **Manage** (Gérer).

Le **gestionnaire ACL** s'ouvre.

Le routeur de premier saut ou l'ITR/ETR pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée; vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.

e) Ajoutez une ACL avec au moins un ACE en fonction du guide de configuration du pare-feu.
f) Si nécessaire, saisissez la **Validation Key** (Clé de validation).

Si vous avez copié une clé chiffrée, cliquez sur le bouton radio **Encrypted** (Chiffré).

g) Cliquez sur **OK**.

Étape 2 Ajoutez une règle de politique de service pour configurer l'inspection LISP :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.
b) Cliquez sur **Add** (ajouter).
c) Dans la page **Service Policy** (Politique de service), appliquez la règle à une interface ou globalement.

Si vous avez une politique de service existante que vous souhaitez utiliser, ajoutez une règle à cette politique. Par défaut, l'ASA comprend une politique globale appelée **global_policy**. Vous pouvez également créer une politique de service par interface si vous ne souhaitez pas appliquer la politique à l'échelle mondiale. L'inspection LISP est appliquée au trafic de manière bidirectionnelle, vous n'avez donc pas besoin d'appliquer la politique de service sur les interfaces source et de destination; tout le trafic qui entre ou sort de l'interface à laquelle vous appliquez la règle est affecté si le trafic correspond à la carte dans les deux sens.

d) Sur la page **Traffic Classification Criteria** (Critères de classification du trafic), cliquez sur **Create a new traffic class** (Créer une nouvelle classe de trafic), et sous **Traffic Match Criteria** (Critères de correspondance du trafic), cochez la case **Source and Destination IP Address (uses ACL)** (Adresse IP source et de destination (utilise ACL)).
e) Cliquez sur **Next** (suivant).
f) Spécifiez le trafic que vous souhaitez inspecter. Vous devez spécifier le trafic entre le routeur de premier saut et l'ITR ou l'ETR sur le port UDP 4342. Les ACL IPv4 et IPv6 sont acceptées.
g) Cliquez sur **Next** (suivant).
h) Sur la page ou l'onglet de l'assistant **Rule Actions** (Actions de règles), sélectionnez l'onglet **Protocol Inspection** (Inspection du protocole).

i) Cochez la case **LISP**.
j) (Facultatif) Cliquez sur **Configure** (Configurer) pour choisir la carte d'inspection que vous avez créée.
k) Cliquez sur **Finish** (Terminer) pour enregistrer la règle de politique de service.

Étape 3 Ajoutez une règle de politique de service pour activer la mobilité des flux pour le trafic critique :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.
b) Cliquez sur **Add** (ajouter).
c) Sur la page **Service Policy** (Politique de service), choisissez la même politique de service que vous avez utilisée pour l'inspection LISP.
d) Sur la page **Traffic Classification Criteria** (Critères de classification du trafic), cliquez sur **Create a new traffic class** (Créer une nouvelle classe de trafic), et sous **Traffic Match Criteria** (Critères de correspondance du trafic), cochez la case **Source and Destination IP Address (uses ACL)** (Adresse IP source et de destination (utilise ACL)).
e) Cliquez sur **Next** (suivant).
f) Spécifiez le trafic opérationnel critique que vous souhaitez réaffecter au site le plus optimal lorsque les serveurs changent de site. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques. Les ACL IPv4 et IPv6 sont acceptées.
g) Cliquez sur **Next** (suivant).
h) Sur la page ou l'onglet de l'assistant **Rule Actions** (Actions de règles), sélectionnez l'onglet **Cluster** (Grappe).
i) Cochez la case **Enable Cluster flow-mobility triggered by LISP EID messages** (Activer la mobilité des flux de grappe déclenchée par les messages LISP EID).
j) Cliquez sur **Finish** (Terminer) pour enregistrer la règle de politique de service.

Étape 4 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)** et cochez la case **Enable Clustering flow mobility** (Activer la mobilité des flux de la grappe).

Étape 5 Cliquez sur **Apply** (Appliquer).

Configurer le VPN de site à site distribué

Par défaut, la grappe utilise le mode VPN de site à site centralisé. Pour profiter de l'évolutivité de la mise en grappe, vous pouvez activer le mode VPN de site à site distribué.

À propos du VPN de site à site distribué

En mode distribué, les connexions VPN IPsec IKEv2 de site à site sont réparties sur les nœuds d'une grappe. La distribution des connexions VPN sur les nœuds d'une grappe permet d'utiliser pleinement la capacité et le débit de la grappe, ce qui augmente considérablement la prise en charge des VPN au-delà des capacités VPN centralisées.

Rôles de connexion du VPN distribué

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée. Lors de l'exécution en mode VPN distribué, les rôles suivants sont affectés aux nœuds de la grappe :

- Propriétaire de session active : le nœud qui reçoit initialement la connexion ou qui a effectué la transition d'une session de sauvegarde en une session active. Le propriétaire conserve l'état et traite les paquets pour toute la session, y compris les tunnels IKE et IPsec et tout le trafic qui leur est associé.
- Propriétaire de la session de sauvegarde : le nœud qui gère la session de sauvegarde pour une session active existante. En cas d'échec du propriétaire de la session active, le propriétaire de la session de secours devient le propriétaire de la session active et une nouvelle session de sauvegarde est établie sur un autre nœud.
- Transmetteur : si le trafic associé à une session VPN est envoyé à un nœud qui n'est pas propriétaire de la session VPN, ce nœud utilisera la liaison de commande de grappe pour transmettre le trafic au nœud propriétaire de la session VPN.
- Orchestrateur : l'orchestrateur (toujours le nœud de contrôle de la grappe) est responsable du calcul des sessions qui se déplaceront et de la destination lors de l'exécution d'une redistribution de sessions actives (ASR). Il envoie une demande au nœud propriétaire X de déplacer N sessions vers le nœud Y. Le nœud X répondra à l'orchestrateur une fois terminé, en précisant le nombre de sessions qu'il a pu déplacer.

Caractéristiques de session du VPN distribué

Les sessions VPN de site à site distribuées présentent les caractéristiques suivantes. Sinon, les connexions VPN se comportent normalement, comme si elles n'étaient pas sur une grappe.

- Les sessions VPN sont réparties dans la grappe au niveau de la session. Cela signifie que le même nœud de grappe gère les tunnels IKE et IPsec et tout leur trafic pour une connexion VPN. Si le trafic de session VPN est envoyé à un nœud de grappe qui ne possède pas cette session VPN, le trafic est transféré au nœud de grappe qui est propriétaire de la session VPN.
- Les sessions VPN ont un ID de session unique dans la grappe. À l'aide de l'ID de session, le trafic est validé, des décisions de transfert sont prises et la négociation IKE est terminée.
- Dans une configuration en étoile avec un VPN de site à site, lorsque les clients se connectent au moyen de la grappe (ce que l'on appelle le hair-pinning), le trafic de session entrant et le trafic de session sortant peuvent se trouver sur des nœuds de grappe différents.
- Vous pouvez exiger que la session de sauvegarde soit allouée sur un module de sécurité dans un autre châssis; cela offre une protection contre les défaillances de châssis. Vous pouvez également choisir d'allouer des sessions de sauvegarde sur n'importe quel nœud de la grappe; cela offre une protection uniquement contre les défaillances de nœuds. Lorsque la grappe contient deux châssis, la sauvegarde sur le châssis distant est fortement conseillée.

Gestion des événements de grappe par le VPN distribué

Événement	VPN distribué
Défaillance de nœud	Pour toutes les sessions actives sur ce nœud défaillant, les sessions de sauvegarde (sur un autre nœud) deviennent actives et les sessions de sauvegarde sont réaffectées sur un autre nœud en fonction de la stratégie de sauvegarde.

Événement	VPN distribué
Défaillance du châssis	Lorsqu'une stratégie de sauvegarde de châssis distant est utilisée, pour toutes les sessions actives sur le châssis défaillant, les sessions de sauvegarde (sur un nœud de l'autre châssis) deviennent actives. Lorsque les nœuds seront remplacés, les sessions de sauvegarde pour ces sessions désormais actives seront réaffectées sur les nœuds du châssis remplacé. Lorsqu'une stratégie de sauvegarde plate est utilisée, si les sessions actives et de sauvegarde se trouvent sur le châssis défaillant, la connexion sera abandonnée. Toutes les sessions actives avec des sessions de sauvegarde sur un nœud de l'autre châssis reviennent à ces sessions. De nouvelles sessions de sauvegarde seront attribuées sur un autre nœud du châssis restant.
Désactiver un nœud de grappe	Pour toutes les sessions actives sur le nœud de grappe qui sont désactivées, les sessions de sauvegarde (sur un autre nœud) deviennent actives et réaffectent les sessions de sauvegarde sur un autre nœud en fonction de la stratégie de sauvegarde.
Joindre un nœud de grappe	Si le mode de grappe VPN sur le nouveau nœud n'est pas distribué, le nœud de contrôle demandera un changement de mode. Une fois que le mode VPN est compatible, le nœud de la grappe se verra attribuer des sessions actives et de sauvegarde dans le flux des opérations normales.

Modifications IPsec IKEv2

IKEv2 est modifié en mode VPN de site à site distribué de la manière suivante :

- Une identité est utilisée à la place des tuples IP/port. Cela permet de prendre des décisions de transfert appropriées sur les paquets et de nettoyer les connexions précédentes qui peuvent se trouver sur d'autres membres de la grappe.
- Les identifiants (SPI) qui identifient une seule session IKEv2 sont des valeurs aléatoires de 8 octets générées localement et uniques dans toute la grappe. Un SPI intègre un horodatage et un ID de nœud de grappe. À la réception d'un paquet de négociation IKE, si la vérification de l'horodatage ou de l'ID du nœud de la grappe échoue, le paquet est abandonné et un message est enregistré pour indiquer la raison.
- Le traitement IKEv2 a été modifié pour empêcher les négociations NAT-T d'échouer en étant réparties entre les membres de la grappe. Un nouveau domaine de classification ASP, *cluster_isakmp_redirect*, et des règles sont ajoutés lorsque IKEv2 est activé sur une interface.

Haute disponibilité pour le VPN de site à site distribué dans la grappe

Les fonctionnalités suivantes offrent une résilience contre la défaillance unique d'un module ou d'un châssis de sécurité :

- Les sessions VPN qui sont sauvegardées sur un autre module de sécurité de la grappe, sur n'importe quel châssis, supportent les défaillances de module de sécurité.
- Les sessions VPN sauvegardées sur un autre châssis supportent les défaillances de châssis.
- Le nœud de contrôle peut changer sans perdre les sessions VPN de site à site.

Si une défaillance supplémentaire se produit avant que la grappe ne soit stable, les connexions peuvent être perdues si les sessions actives et de secours se trouvent sur les nœuds défaillants.

Toutes les tentatives sont faites pour assurer qu'aucune session ne soit perdue lorsqu'un nœud quitte la grappe de manière progressive, comme la désactivation du mode grappe VPN, le rechargement d'un nœud de grappe et d'autres modifications de châssis anticipées. Pendant ce type d'opérations, les sessions ne seront pas perdues tant que la grappe aura le temps de rétablir les sauvegardes de sessions entre les opérations. Si une sortie progressive est déclenchée sur le dernier nœud de la grappe, elle supprimera rapidement les sessions existantes.

CMPv2

Le certificat d'identification et les paires de clés CMPv2 sont synchronisés sur les nœuds de la grappe. Cependant, seul le nœud de contrôle de la grappe renouvelle automatiquement et resaisit le certificat CMPv2. Le nœud de contrôle synchronise ces nouveaux certificats d'identification et clés avec tous les nœuds de la grappe lors d'un renouvellement. De cette façon, tous les nœuds de la grappe utilisent les certificats CMPv2 pour l'authentification, et tous les nœuds sont capables de prendre le relais en tant que nœud de contrôle.

Licences pour le VPN de site à site distribué

Une licence d'opérateur est requise pour le VPN de site à site distribué, sur chaque membre de la grappe.

Chaque connexion VPN nécessite deux sessions sous licence *Other VPN* (Autre VPN) (la licence *Other VPN* (Autre VPN) fait partie de la licence *Essentials*), une pour la session active et une pour la session de secours. La capacité maximale de sessions VPN de la grappe ne peut pas dépasser la moitié de la capacité sous licence en raison de l'utilisation de deux licences pour chaque session.

Conditions préalables au VPN de site à site distribué

Prise en charge des modèles

- Firepower 9300
- Maximum de 6 modules sur 2 châssis. Vous pouvez installer un nombre différent de modules de sécurité dans chaque châssis, mais nous conseillons une répartition égale.

Maximum de sessions VPN

Chaque module de sécurité prend en charge jusqu'à 6 000 sessions VPN pour un maximum d'environ 36 000 sessions sur 6 nœuds.

Le nombre réel de sessions prises en charge sur un nœud de grappe est déterminé par la capacité de la plateforme, les licences allouées et l'allocation des ressources par contexte. Lorsque l'utilisation est proche de la limite, il peut arriver que la création de sessions échoue, même si la capacité maximum n'a pas été atteinte sur chaque nœud de la grappe. En effet, l'allocation de sessions actives est déterminée par une commutation externe et l'allocation de sessions de secours est déterminée par un algorithme de grappe interne. Nous invitons les clients à dimensionner leur utilisation en conséquence et à prévoir une marge pour une répartition inégale.

Lignes directrices relatives au VPN de site à site distribué

Mode pare-feu

Le VPN de site à site distribué est pris en charge en mode routé uniquement.

Mode contextuel

Le VPN de site à site distribué fonctionne à la fois en mode de contexte unique et en mode de contexte multiple. Cependant, en mode de contexte multiple, la redistribution des sessions actives est effectuée au niveau du système, et non au niveau du contexte. Cela empêche une session active associée à un contexte de se déplacer vers un membre de grappe qui contient des sessions actives associées à un contexte différent, créant ainsi une charge non pris en charge.

Inspections non prises en charge

Les types d'inspections suivants ne sont pas pris en charge ou sont désactivés en mode VPN de site à site distribué :

- CTIQBE
- DCERPC
- H323, H225 et RAS
- Intercommunication IPsec
- MGCP
- MMP
- NetBIOS
- PPTP
- RADIUS
- RSH
- RTSP
- SCCP (Skinny)
- SunRPC
- TFTP
- WAAS
- WCCP
- XDMCP

Directives supplémentaires

- Seul le VPN de site à site IKEv2 IPsec est pris en charge en mode VPN de site à site distribué. IKEv1 n'est pas pris en charge. Le VPN de site à site IKEv1 est pris en charge en mode VPN centralisé.
- La mise en grappe inter-sites n'est pas prise en charge.
- La PAT dynamique n'est pas disponible en mode VPN de site à site distribué.

Activer le VPN de site à site distribué

Activez le VPN de site à site distribué pour profiter de l'évolutivité de la mise en grappe pour les sessions VPN.

Remarque Le passage du mode VPN entre centralisé et distribué nécessite le rechargement de tous les nœuds de la grappe. La modification du mode de sauvegarde est dynamique et ne mettra pas fin aux sessions.

Avant de commencer

Configurez le VPN de site à site en fonction du guide de configuration de VPN.

Procédure

Étape 1 Choisissez **Configuration > Device Management (Gestion des périphériques) > High Availability and Scalability (Haute disponibilité et évolutivité) > ASA Cluster (Grappe ASA)**.

Étape 2 Dans la zone **VPN Cluster Mode** (Mode de grappe VPN), choisissez le **VPN Mode** (Mode VPN) pour la grappe, **Centralized** (Centralisé) ou **Distributed** (Distribué).

Étape 3 Choisissez le **Backup Distribution Mode** (Mode de distribution de la sauvegarde), **Flat** (Plat) ou **Remote-chassis** (Châssis distant).

En mode de sauvegarde **plate**, des sessions de veille sont établies sur n'importe quel autre nœud de la grappe. Cela protégera les utilisateurs contre les défaillances de module; cependant, la protection contre les défaillances de châssis n'est pas garantie.

En mode de sauvegarde du **châssis distant**, des sessions de veille sont établies sur un nœud d'un autre châssis de la grappe. Cela protégera les utilisateurs contre les défaillances de module et de châssis.

Si le **châssis distant** est configuré dans un environnement de châssis unique (configuré intentionnellement ou à la suite d'une défaillance), aucune sauvegarde ne sera créée avant qu'un autre châssis rejoigne la grappe.

Étape 4 Cliquez sur **Apply** (Appliquer).

Vous serez invité à procéder au rechargement. Ce paramètre est répliqué sur tous les nœuds de données avant le rechargement; tous les nœuds de la grappe se rechargeront.

Redistribuer les sessions du VPN S2S distribué

La redistribution des sessions actives redistribue la charge des sessions VPN actives sur les nœuds de la grappe. En raison de la nature dynamique des sessions de début et de fin, la redistribution des sessions actives permet d'équilibrer au mieux les sessions sur tous les nœuds de la grappe. Des actions de redistribution répétées optimiseront l'équilibre.

La redistribution peut être exécutée à tout moment, mais il est conseillé de la réaliser après toute modification de topologie dans la grappe et après qu'un nouveau nœud a rejoint la grappe. L'objectif de la redistribution est de créer une grappe VPN stable. Une grappe VPN stable a un nombre presque égal de sessions actives et de sauvegarde sur les nœuds.

Pour déplacer une session, la session de sauvegarde devient active et un autre nœud est sélectionné pour héberger une nouvelle session de sauvegarde. Le déplacement des sessions dépend de l'emplacement de la sauvegarde de la session active et du nombre de sessions actives déjà sur ce nœud de sauvegarde en particulier. Si le nœud de session de sauvegarde ne peut pas héberger la session active pour une raison quelconque, le nœud d'origine reste propriétaire de la session.

En mode de contexte multiple, la redistribution des sessions actives est effectuée au niveau du système, et non au niveau du contexte individuel. Elle ne se fait pas au niveau du contexte, car une session active dans un contexte peut déplacer un nœud qui contient de nombreuses sessions actives dans un contexte différent, créant ainsi une charge plus importante sur ce nœud de grappe.

Avant de commencer

- Activez les journaux système si vous souhaitez superviser l'activité de redistribution.
- Cette procédure doit être effectuée sur l'unité de contrôle de la grappe.

Procédure

Étape 1 Choisissez **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > ASA Cluster (Grappe ASA) > Cluster Summary (Résumé de la grappe) > VPN Cluster Summary (Résumé de la grappe VPN)** pour afficher la distribution des sessions actives et de sauvegarde dans la grappe.

Selon le nombre de sessions à redistribuer et la charge sur la grappe, cela peut prendre un certain temps. Les journaux système contenant les expressions suivantes (et d'autres détails sur le système non affichés ici) sont fournis au fur et à mesure que l'activité de redistribution se produit :

Expression du journal système	Notes
Redistribution de la session VPN démarrée	Nœud de contrôle uniquement
Demande envoyée pour déplacer *nombre* sessions de *orig-member-name* à *dest-member-name*	Nœud de contrôle uniquement
Échec de l'envoi du message de redistribution de session à *member-name*	Nœud de contrôle uniquement
Demande reçue pour déplacer *nombre* sessions de *orig-member-name* à *dest-member-name*	Nœud de données uniquement
Déplacement de *nombre* sessions à *member-name*	Le nombre de sessions actives déplacées vers la grappe nommée.
Échec de la réception de la réponse de déplacement de session depuis *dest-member-name*	Nœud de contrôle uniquement
Session VPN terminée	Nœud de contrôle uniquement
Modification de la topologie de grappe détectée. Redistribution de la session VPN abandonnée.	

Étape 2 Cliquez sur **Re-Distribute** (Redistribuer).

Étape 3 Actualisez **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > ASA Cluster (Grappe ASA) > Cluster Summary (Résumé de la grappe) > VPN Cluster Summary (Résumé de la grappe VPN)** pour afficher les résultats de l'activité de redistribution.

Si votre redistribution a réussi et qu'il n'y a eu aucune activité substantielle de système ou de session, votre système sera équilibré et cette action est terminée.

Sinon, répétez le processus de redistribution pour obtenir un système équilibré et stable.

FXOS : supprimer un nœud de la grappe

Les sections suivantes décrivent comment supprimer des nœuds de façon temporaire ou permanente de la grappe.

Suppression temporaire

Un nœud de grappe sera automatiquement supprimé de la grappe en raison d'une défaillance matérielle ou réseau, par exemple. Cette suppression est temporaire jusqu'à ce que les conditions soient rectifiées, et qu'il puisse rejoindre la grappe. Vous pouvez également désactiver manuellement la mise en grappe.

Pour vérifier si un appareil se trouve actuellement dans la grappe, vérifiez l'état de la grappe dans la page Firewall Chassis Manager **Logical Devices**(périphériques logiques) : :



- Disable clustering in the application (désactivez la mise en grappe dans l'application) : Vous pouvez désactiver la mise en grappe à l'aide de l'interface de ligne de commande de l'application. Saisissez la commande **cluster remove unit** *name* pour supprimer tout nœud autre que celui auquel vous êtes connecté. La configuration de démarrage reste inchangée, ainsi que la dernière configuration synchronisée à partir du nœud de contrôle, afin que vous puissiez rajouter le nœud ultérieurement sans perdre votre configuration. Si vous saisissez cette commande sur un nœud de données pour supprimer le nœud de contrôle, un nouveau nœud de contrôle est élu.

  Lorsqu'un périphérique devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de la configuration de démarrage. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), l'interface de gestion est désactivée.

  Pour réactiver la mise en grappe, saisissez le **cluster group** *name* sur l'ASA, puis **enable**.

- Désactivez l'instance d'application : Dans la page Firewall Chassis Manager dans la page **Logical Devices** (Périphériques logiques), cliquez sur **Curseur activé** (). Vous pourrez la réactiver ultérieurement à l'aide de **Curseur désactivé** ().
- Arrêtez le security module/engine : Dans Firewall Chassis Manager sur la page **Security Module/Engine** (module/moteur de sécurité), cliquez sur l'icône **Mettre hors tension**.
- Arrêtez le châssis : dans le Firewall Chassis Manager sur la page d'**aperçu**, cliquez sur l'icône**Arrêt**.

Suppression permanente

Vous pouvez supprimer définitivement un nœud de grappe en utilisant les méthodes suivantes.

- Supprimez le périphérique logique :Dans la zone Firewall Chassis Manager de la page **Logical Devices** (Périphériques logiques), cliquez sur **Supprimer** (). Vous pouvez ensuite déployer un périphérique logique autonome, une nouvelle grappe ou même ajouter un nouveau périphérique logique à la même grappe.
- Supprimez le châssis ou le module de sécurité du service : si vous mettez un périphérique hors du service, vous pouvez ajouter du matériel de remplacement en tant que nouveau nœud de la grappe.

ASA : Gérer les membres de la grappe

Après avoir déployé la grappe, vous pouvez modifier la configuration et gérer les membres de celle-ci.

Devenir un membre inactif

Pour devenir un membre inactif de la grappe, désactivez la mise en grappe sur le nœud tout en laissant intacte la configuration de mise en grappe.



Remarque Lorsqu'un ASA devient inactif (soit manuellement, soit à la suite d'un échec du contrôle d'intégrité), toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe; ou vous pouvez supprimer complètement le nœud de la grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), alors l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Avant de commencer

- Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système dans le volet Configuration > Device List (Liste des périphériques) et double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)**.

Étape 2 Décochez la case **Participer à la grappe ASA**.

Remarque Ne décochez pas la case **Configurer les paramètres de grappe ASA**. Cette action efface toute la configuration de la grappe et désactive également toutes les interfaces, y compris l'interface de gestion à laquelle ASDM est connecté. Pour rétablir la connectivité dans ce cas, vous devez accéder à l'interface de ligne de commande au niveau du port de console.

Étape 3 Cliquez sur **Apply** (Appliquer).

Désactiver une unité de données de l'unité de contrôle

Pour désactiver un nœud de données, procédez comme suit.

Remarque Lorsqu'un ASA devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Avant de commencer

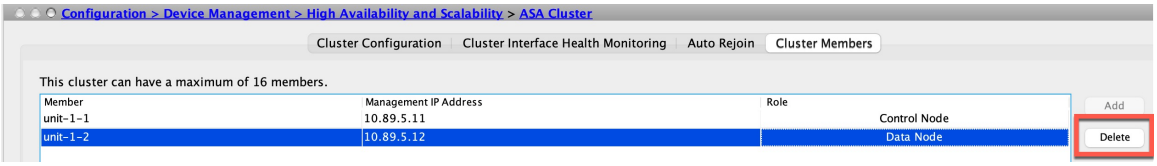
Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système dans le **volet Configuration > Device List (Liste des périphériques)** et double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Members (Membres de la grappe)**.

Étape 2 Sélectionnez le nœud de données que vous souhaitez supprimer et cliquez sur **Delete** (Supprimer).

Illustration 61 : Supprimer un nœud



La configuration de démarrage du nœud de données reste inchangée afin que vous puissiez rajouter le nœud de données ultérieurement sans perdre votre configuration.

Étape 3 Cliquez sur **Apply** (Appliquer).

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement un membre, vous devez rejoindre manuellement la grappe.

Avant de commencer

- Vous devez utiliser le port de console pour réactiver la mise en grappe. Les autres interfaces sont fermées. L'exception est que si vous avez désactivé manuellement la mise en grappe dans ASDM, vous pouvez réactiver la mise en grappe dans ASDM si vous n'avez pas enregistré la configuration et ne l'avez pas rechargée. Après le rechargement, l'interface de gestion est désactivée. L'accès à la console est donc la seule méthode pour réactiver la mise en grappe.
- Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système dans le **volet Configuration > Device List (Liste des périphériques)** et double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.
- Assurez-vous que le problème est résolu avant d'essayer de rejoindre la grappe.

Procédure

Étape 1 Si vous avez toujours l'accès à ASDM, vous pouvez réactiver la mise en grappe dans ASDM en connectant ASDM au nœud que vous souhaitez réactiver.

Vous ne pouvez pas réactiver la mise en grappe pour un nœud de données à partir du nœud de contrôle, sauf si vous l'ajoutez en tant que nouveau membre.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**.
b) Cochez la case **Participate in ASA cluster** (Participer à la grappe ASA).
c) Cliquez sur **Apply** (Appliquer).

Étape 2 Si vous ne pouvez pas utiliser ASDM : Sur la console, passez en mode de configuration de grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 3 Activez la mise en grappe.

enable

Changer l'unité de contrôle



Mise en garde La méthode recommandée pour changer le nœud de contrôle est de désactiver la mise en grappe sur celui-ci en attendant un nouveau choix de contrôle, puis de réactiver la mise en grappe. Si vous devez spécifier le nœud exact que vous souhaitez voir devenir le nœud de contrôle, utilisez la procédure décrite dans cette section. Notez toutefois que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle à l'aide de cette procédure, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Pour modifier le nœud de contrôle, procédez comme suit.

Avant de commencer

Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système dans le volet Configuration > Device List (Liste des périphériques) et double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Summary (Résumé de la grappe)**.

Étape 2 Dans la liste déroulante, choisissez un nœud de données pour devenir le contrôle et cliquez sur le bouton pour en faire le nœud de contrôle.

Étape 3 Vous êtes invité à confirmer le changement de nœud de contrôle. Cliquez sur **Oui**.

Étape 4 Quittez ASDM et reconnectez-vous en utilisant l'adresse IP de la grappe principale.

Exécuter une commande à l'échelle de la grappe

Pour envoyer une commande à tous les membres de la grappe ou à un membre en particulier, procédez comme suit. L'envoi d'une commande **show** à tous les membres collecte toutes les sorties et les affiche sur la console de l'unité actuelle. (Notez qu'il existe également des commandes d'affichage (show) que vous pouvez saisir sur l'unité de contrôle pour afficher les statistiques à l'échelle de la grappe.) D'autres commandes, telles que **capture** et **copy**, peuvent également profiter d'une exécution à l'échelle de la grappe.

Avant de commencer

Effectuez cette procédure au niveau de l'outil d'interface de ligne de commande : choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

Procédure

Envoyez une commande à tous les membres ou, si vous spécifiez le nom de l'unité, à un membre en particulier :

cluster exec [unit *unit_name*] *command*

Exemple :

```
cluster exec show xlate
```

Pour afficher les noms des membres, saisissez **cluster exec unit ?** (pour afficher tous les noms à l'exception de l'unité actuelle) ou saisissez la commande **show cluster info**.

Exemples

Pour copier simultanément le même fichier de capture de toutes les unités de la grappe vers un serveur TFTP, saisissez la commande suivante sur l'unité de contrôle :

```
cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Plusieurs fichiers PCAP, un pour chaque unité, sont copiés sur le serveur TFTP. Le nom du fichier de capture de destination est automatiquement associé au nom de l'unité, par exemple capture1_asa1.pcap, capture1_asa2.pcap, etc. Dans cet exemple, asa1 et asa2 sont des noms d'unités de grappe.

L'exemple de sortie suivant pour la commande **cluster exec show memory** affiche les renseignements sur la mémoire pour chaque membre de la grappe :

```
cluster exec show memory
unit-1-1(LOCAL):*******************************************************
Free memory:      108724634538 bytes (92%)
Used memory:        9410087158 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-3:*******************************************************************
Free memory:      108749922170 bytes (92%)
Used memory:        9371097334 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-2:*******************************************************************
Free memory:      108426753537 bytes (92%)
Used memory:        9697869087 bytes ( 8%)
-------------     ------------------
```

```
Total memory:     118111600640 bytes (100%)
```

ASA : supervision de la grappe ASA sur le Châssis Firepower 4100/9300

Vous pouvez superviser et dépanner l'état de la grappe et les connexions.



Remarque Lors de la comparaison des paquets sur la liaison de commande de grappe dans ASA et FXOS, le nombre de paquets FXOS est supérieur à ce qui est affiché dans ASA. Dans ASA, seuls les paquets destinés à l'adresse IP de la liaison de commande de grappe sont comptabilisés dans les paquets d'entrée. Les paquets transmis, qui sont réinjectés dans les interfaces de données, ne sont comptabilisés que dans les statistiques *d'entrée* des interfaces de données et les statistiques *de sortie* de la liaison de commande de grappe.

Supervision de l'état de la grappe

Consultez les écrans suivantes pour superviser l'état de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Cluster Summary (Résumé de la grappe)**

  Ce volet affiche des renseignements sur la grappe concernant l'unité à laquelle vous êtes connecté, ainsi que les autres unités de la grappe. Vous pouvez également modifier l'unité principale à partir de ce volet.

- **Tableau de bord de la grappe**

  Sur la page d'accueil de l'unité principale, vous pouvez superviser la grappe à l'aide des tableaux de bord de grappe et de pare-feu de grappe.

Capture des paquets à l'échelle de la grappe

Consultez l'écran suivante pour capturer des paquets dans une grappe :

Wizards (Assistants) > Packet Capture Wizard (Assistant de capture de paquets)

Pour prendre en charge le dépannage à l'échelle de la grappe, vous pouvez activer la capture du trafic spécifique à la grappe sur le nœud de contrôle, qui est ensuite automatiquement activée sur tous les nœuds de données de la grappe.

Supervision des ressources de la grappe

Consultez les écrans suivants pour surveiller les ressources de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > System Resources Graphs (Graphiques de ressources système) > CPU (Processeur)**

  Ce volet vous permet de créer des graphiques ou des tableaux montrant l'utilisation du processeur sur les membres de la grappe.

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > System Resources Graphs (Graphiques de ressources système) > Memory (Mémoire)**.

  Ce volet vous permet de créer des graphiques ou des tableaux montrant la mémoire libre et la mémoire utilisée sur les membres de la grappe.

Supervision du trafic de la grappe

Consultez les écrans suivants pour superviser le trafic de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Trafic Graphs (Graphiques du trafic) > Connections (Connexions)**.

  Ce volet vous permet de créer des graphiques ou des tableaux montrant les connexions entre les membres de la grappe.

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Trafic Graphs (Graphiques du trafic) > Throughput (Débit)**.

  Ce volet vous permet de créer des graphiques ou des tableaux montrant le débit du trafic entre les membres de la grappe.

- **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Load-Monitoring (Supervision de la charge de la grappe)**

  Cette section comprend les volets **Load Monitor-Information** (Renseignements sur le moniteur de charge) et **Load-Monitor Details** (Détails du moniteur de charge). **Load Monitor-Information** (Renseignements sur le moniteur de charge) affiche la charge de trafic pour les membres de la grappe pour le dernier intervalle ainsi que la moyenne du nombre total d'intervalles configurés (30 par défaut). Utilisez le volet **Load-Monitor Details** (Détails du moniteur de charge) pour afficher la valeur de chaque mesure à chaque intervalle.

Supervision de la liaison de commande de grappe

Consultez l'écran suivant pour superviser l'état de la grappe :

Monitoring (Supervision) > Properties (Propriétés) > System Resources Graphs (Graphiques des ressources du système) > Cluster Control Link (Liaison de commande de grappe).

Ce volet vous permet de créer des graphiques ou des tableaux indiquant l'utilisation de la capacité de réception et de transmission de la liaison de commande de grappe.

Supervision du routage de la grappe

Consultez l'écran suivant pour le routage de la grappe :

- **Monitoring (Supervision)** > **Routing (Routage)** > **LISP-EID Table (Tableau LISP-EID)**

  Affiche le tableau EID de l'ASA qui indique les EID et les ID de site.

Supervision du VPN S2S distribué

Consultez les écrans suivants pour superviser l'état de la grappe VPN :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > ASA Cluster (Grappe ASA) > Cluster Summary (Résumé de la grappe) > VPN Cluster Summary (Résumé de la grappe VPN)**

  Affiche la répartition de la session dans la grappe et vous permet de redistribuer les sessions.

- **Monitoring (Supervision) > VPN > VPN Statistics (Statistiques de VPN) > Sessions**

  Les nœuds de contrôle et de données de la grappe sont répertoriés. Cliquez sur n'importe quel nœud pour obtenir les détails.

Configuration de la journalisation pour la mise en grappe

Consultez l'écran suivante pour configurer la journalisation pour la mise en grappe :

Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Setup (Configuration du journal système)

Chaque nœud de la grappe génère des messages de journal système de manière indépendante. Vous pouvez pour générer des messages de journal système avec des ID de périphérique identiques ou différents afin de faire apparaître les messages comme provenant de nœuds identiques ou différents dans la grappe.

Dépannage du VPN S2S distribué

Notifications de VPN distribuées

Vous recevrez des messages contenant les expressions identifiées lorsque les situations d'erreur suivantes se produisent sur une grappe exécutant le VPN distribué :

Situation	Notification

Si un nœud de données de grappe existant ou en cours de connexion n'est pas en mode VPN distribué lors de la tentative de connexion à la grappe :	`Nouveau membre de la grappe (member-name) refusé en raison d'une incompatibilité de mode VPN.`
	et
	`Le nœud de contrôle (control-name) refuse la demande d'inscription de l'unité (unit-name) pour la raison suivante : les capacités du mode VPN ne sont pas compatibles avec la configuration du nœud de contrôle`

Si la licence n'est pas configurée correctement sur un membre de la grappe pour le VPN distribué :	`ERREUR : le nœud de contrôle a demandé le changement de mode VPN de la grappe sur distribué. Impossible de changer de mode en raison d'une licence d'opérateur manquante.`

Si l'horodatage ou l'ID de membre est non valide dans le SPI d'un paquet IKEv2 reçu :	`SPI expiré reçu`
	ou
	`SPI corrompu détecté`

Si la grappe ne peut pas créer de session de sauvegarde :	`Échec de la création de la sauvegarde pour une session IKEv2.`

Situation	Notification
Erreur de traitement du contact initial IKEv2 :	`Négociation IKEv2 abandonnée en raison d'une ERREUR : session de sauvegarde obsolète trouvée sur la sauvegarde`
Problèmes de redistribution :	`Échec de l'envoi du message de redistribution de session à member-name` `Échec de la réception de la réponse de déplacement de session de member-name (nœud de contrôle uniquement)`
Si la topologie change lors de la redistribution des sessions :	`Modification de la topologie de grappe détectée. Redistribution de la session VPN abandonnée.`

Vous pouvez rencontrer l'une des situations suivantes :

- Les sessions VPN de site à site sont distribuées à un seul des châssis d'une grappe lorsque le commutateur Nexus 7K est configuré avec un port de couche 4 comme algorithme d'équilibrage de charges à l'aide de la commande **port-channel load-balance src-dst l4port**. Voici un exemple d'allocation de session de grappe :

```
SSP-Cluster/data node(cfg-cluster)# show cluster vpn-sessiondb distribution
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
5(2501)
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

Étant donné que le VPN IKEv2 de site à site utilise le port 500 pour les ports source et de destination, les paquets IKE ne sont envoyés qu'à l'une des liaisons du canal de port connecté entre le Nexus 7K et le châssis.

Modifiez l'algorithme d'équilibrage de charges Nexus 7K sur l'adresse IP et le port de couche 4 à l'aide de **port-channel load-balance src-dst ip-l4port**. Ensuite, les paquets IKE sont envoyés à toutes les liaisons et donc à tous les nœuds.

Pour un ajustement plus immédiat, sur le nœud de contrôle de la grappe, exécutez : **cluster redistribute vpn-sessiondb** pour redistribuer les sessions VPN actives aux nœuds de grappe des autres châssis.

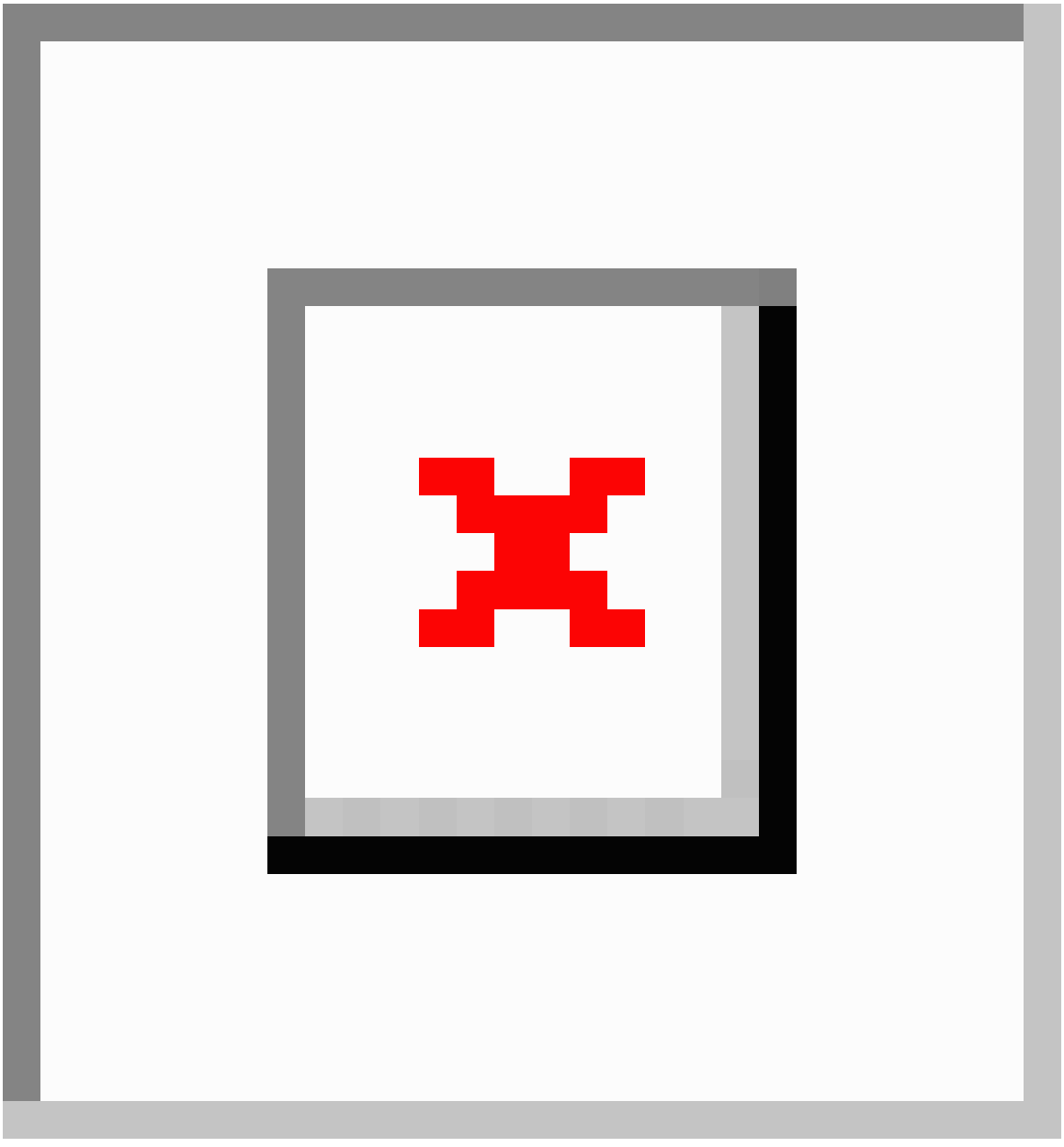
Exemples de mise en grappe d'ASA

Ces exemples comprennent des déploiements typiques.

Pare-feu sur une seule interface

Le trafic de données de différents domaines de sécurité est associé à différents VLAN. Par exemple, VLAN 10 pour le réseau interne et VLAN 20 pour le réseau externe. Chaque ASA dispose d'un seul port physique connecté au commutateur ou routeur externe. Le regroupement de liaisons est activé de sorte que tous les paquets sur la liaison physique soient encapsulés dans une norme 802.1q. L'ASA sert de pare-feu entre le VLAN 10 et le VLAN 20.

Lorsque vous utilisez des EtherChannels étendus, toutes les liaisons de données sont regroupées dans un seul EtherChannel du côté du commutateur. Si l'ASA n'est plus disponible, le commutateur rééquilibre le trafic entre les unités restantes.



Mode d'interface sur chaque unité

```
cluster interface-mode spanned force
```

Configuration de démarrage de l'unité de contrôle de l'unité 1

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa1
cluster-interface ethernet1/8 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

Configuration de démarrage de l'unité de données de l'unité 2

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa2
cluster-interface ethernet1/8 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-data-node
```

Configuration de démarrage de l'unité de données de l'unité 3

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa3
cluster-interface ethernet1/8 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-data-node
```

Configuration de l'interface de l'unité de contrôle

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
```

```
no shutdown

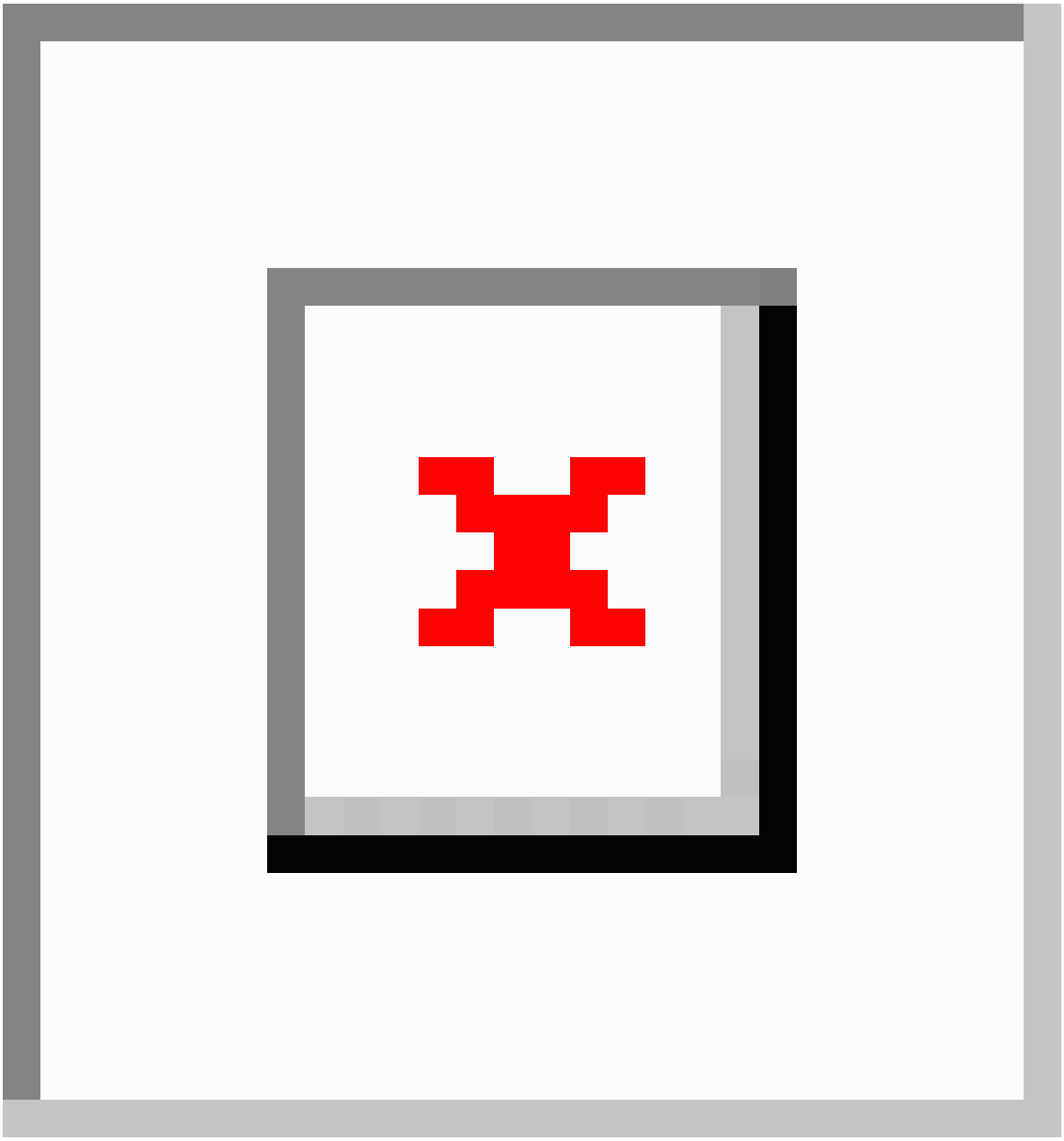
interface ethernet1/1
channel-group 1 mode active
no shutdown

interface port-channel 1

interface port-channel 1.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE

interface port-channel 1.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

Ségrégation du trafic



Comme le montre le diagramme ci-dessus, il y a un EtherChannel étendu sur le côté gauche qui se connecte au commutateur interne et l'autre sur le côté droit au commutateur externe. Vous pouvez également créer des sous-interfaces VLAN sur chaque EtherChannel, au besoin.

Mode d'interface sur chaque unité

```
cluster interface-mode spanned force
```

Configuration de démarrage de l'unité de contrôle de l'unité 1

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa1
 cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
 priority 1
 key chuntheunavoidable
 enable noconfirm
```

Configuration de démarrage de l'unité de données de l'unité 2

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa2
 cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
 priority 2
 key chuntheunavoidable
 enable as-data-node
```

Configuration de démarrage de l'unité de données de l'unité 3

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa3
 cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
 priority 3
 key chuntheunavoidable
 enable as-data-node
```

Configuration de l'interface de l'unité de contrôle

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
 nameif management
 ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
 ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
 security-level 100
 management-only
 no shutdown

interface ethernet 1/8
 channel-group 2 mode active
 no shutdown

interface port-channel 2
 nameif inside
 ip address 10.10.10.5 255.255.255.0
 ipv6 address 2001:DB8:1::5/64
 mac-address 000C.F142.4CDE

interface ethernet 2/1
 channel-group 3 mode active
 no shutdown

interface port-channel 3
 nameif outside
 ip address 209.165.201.1 255.255.255.224
 ipv6 address 2001:DB8:2::8/64
 mac-address 000C.F142.5CDE
```

Configuration OTV pour la mise en grappe inter-sites en mode routé

La réussite de la mise en grappe inter-sites pour le mode routé avec les EtherChannels étendus dépend de la configuration et de la supervision appropriées de l'OTV. L'OTV joue un rôle majeur en transférant les paquets sur l'interface DCI. L'OTV transfère les paquets de monodiffusion sur l'interface DCI uniquement lorsqu'il apprend l'adresse MAC dans sa table de transfert. Si l'adresse MAC n'est pas apprise dans la table de transfert OTV, il abandonnera les paquets de monodiffusion.

Exemple de configuration OTV

```
//Sample OTV config:
//3151 - Inside VLAN, 3152 - Outside VLAN, 202 - CCL VLAN
//aaaa.1111.1234 - ASA inside interface global vMAC
//0050.56A8.3D22 - Server MAC

feature ospf
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
```

```
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

Modifications du filtre OTV requises en raison d'une défaillance du site

Si un site tombe en panne, les filtres doivent être supprimés de l'OTV, car il n'est plus nécessaire de bloquer l'adresse MAC globale. Certaines configurations supplémentaires sont nécessaires.

Vous devez ajouter une entrée statique pour l'adresse MAC globale ASA sur le commutateur OTV dans le site qui est fonctionnel. Cette entrée permettra à l'OTV à l'autre extrémité d'ajouter ces entrées sur l'interface de superposition. Cette étape est nécessaire, car si le serveur et le client ont déjà l'entrée ARP pour l'ASA, ce qui est le cas pour les connexions existantes, ils n'enverront pas à nouveau l'ARP. Par conséquent, l'OTV n'aura pas la possibilité d'apprendre l'adresse MAC globale ASA dans sa table de transfert. Étant donné que l'OTV n'a pas l'adresse MAC globale dans sa table de transfert et que, conformément à sa conception, il ne diffusera pas de paquets de monodiffusion sur l'interface de superposition, il abandonnera les paquets de monodiffusion à l'adresse MAC globale du serveur, et les connexions existantes seront interrompues.

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

Lorsque l'autre site est restauré, vous devez ajouter de nouveau les filtres et supprimer cette entrée statique sur l'OTV. Il est très important d'effacer le tableau des adresses MAC dynamiques sur les deux OTV pour effacer l'entrée de superposition pour l'adresse MAC globale.

Effacement du tableau d'adresses MAC

Lorsqu'un site tombe en panne et qu'une entrée statique pour l'adresse MAC globale est ajoutée à l'OTV, vous devez laisser l'autre OTV apprendre l'adresse MAC globale sur l'interface de superposition. Une fois l'autre site rétabli, ces entrées doivent être effacées. Assurez-vous d'effacer la table d'adresses MAC pour vous assurer que l'OTV ne conserve aucune de ces entrées dans sa table de transfert.

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
```

```
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

Supervision du cache OTV ARP

Le service OTV gère un cache ARP pour mandataire ARP pour les adresses IP qu'il a apprises sur l'interface OTV.

```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

Exemples de mise en grappe inter-sites

Les exemples suivants montrent les déploiements de grappe pris en charge.

Exemple de mode de routage EtherChannel étendu avec des adresses MAC et IP propres au site

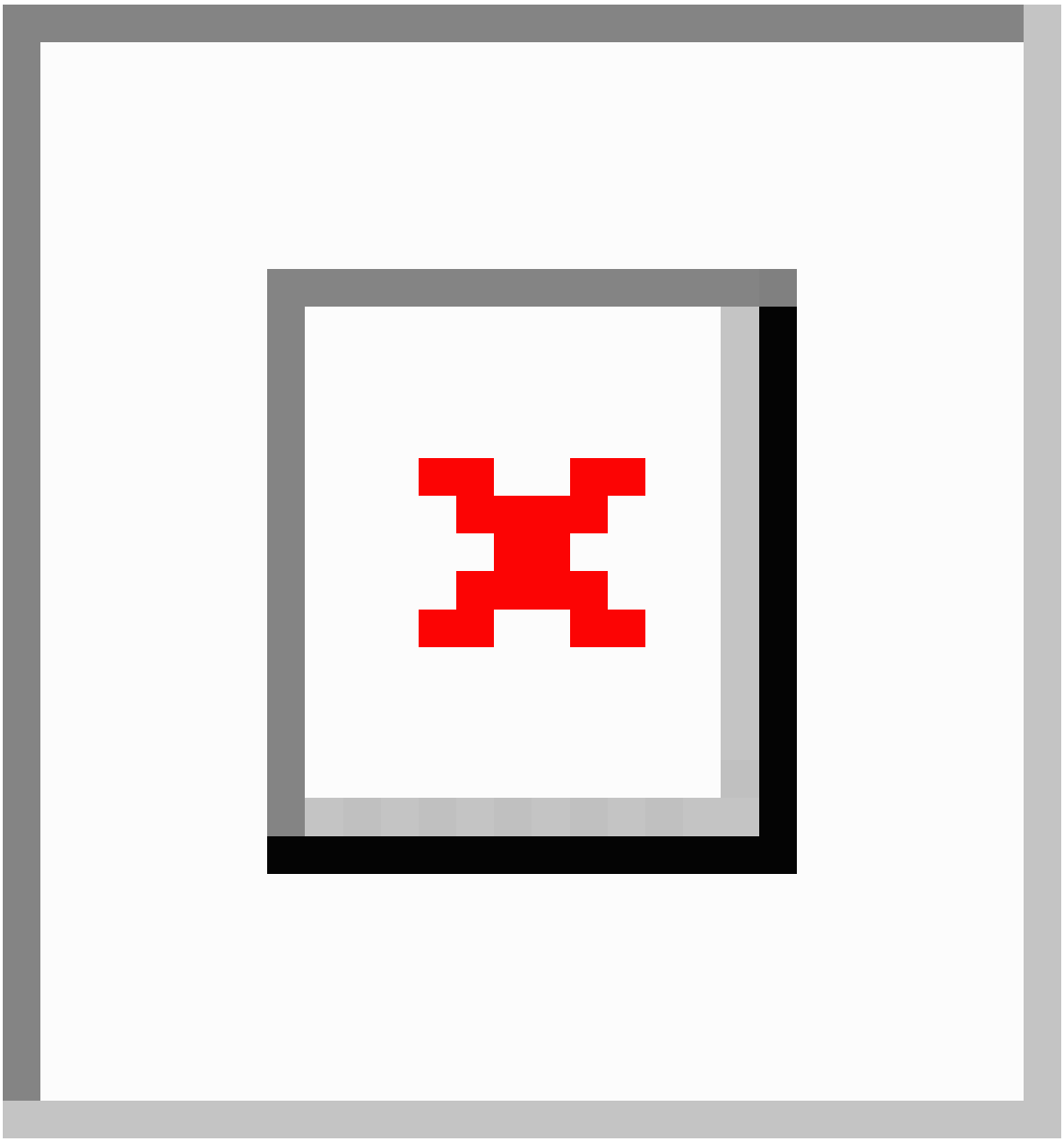
L'exemple suivant montre deux membres de la grappe dans chacun des deux centres de données, placés entre le routeur de passerelle et un réseau interne sur chaque site (insertion est-ouest). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs locaux en utilisant des EtherChannels étendus pour le réseau interne et externe. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Les VLAN de données sont étendus entre les sites à l'aide de la virtualisation du transport par superposition (OTV) (ou d'un outil similaire). Vous devez ajouter des filtres bloquant l'adresse MAC globale pour empêcher le trafic de traverser l'interface DCI vers l'autre site lorsqu'il est destiné à la grappe. Si les nœuds de la grappe d'un site deviennent inaccessibles, vous devez supprimer les filtres pour que le trafic puisse être dirigé vers les nœuds de la grappe de l'autre site. Vous devez utiliser les adresses VACL pour filtrer l'adresse MAC globale.Pour certains commutateurs, comme le Nexus avec la carte de ligne de la gamme F3, vous devez également utiliser l'inspection ARP pour bloquer les paquets ARP de l'adresse MAC globale. L'inspection ARP nécessite que vous définissiez à la fois l'adresse MAC et l'adresse IP du site sur l'ASA. Si vous configurez uniquement l'adresse MAC du site N'oubliez pas de désactiver l'inspection ARP.

La grappe sert de passerelle pour les réseaux internes. Le MAC virtuel global, qui est partagé sur tous les nœuds de la grappe, est utilisé uniquement pour recevoir des paquets. Les paquets sortants utilisent une adresse MAC spécifique au site pour chaque grappe de contrôleurs de domaine. Cette fonctionnalité empêche les commutateurs d'apprendre la même adresse MAC globale à partir des deux sites sur deux ports différents, ce qui entraîne une oscillation MAC; au lieu de cela, ils connaissent uniquement l'adresse MAC du site.

Dans ce scénario :

- Tous les paquets de sortie envoyés par la grappe utilisent l'adresse MAC du site et sont localisés dans le centre de données.
- Tous les paquets entrants vers la grappe sont envoyés à l'aide de l'adresse MAC globale, de sorte qu'ils peuvent être reçus par n'importe quel nœud des deux sites; les filtres de l'OTV localisent le trafic dans le centre de données.



Exemple intersites nord-sud de mode transparent de l'EtherChannel étendu

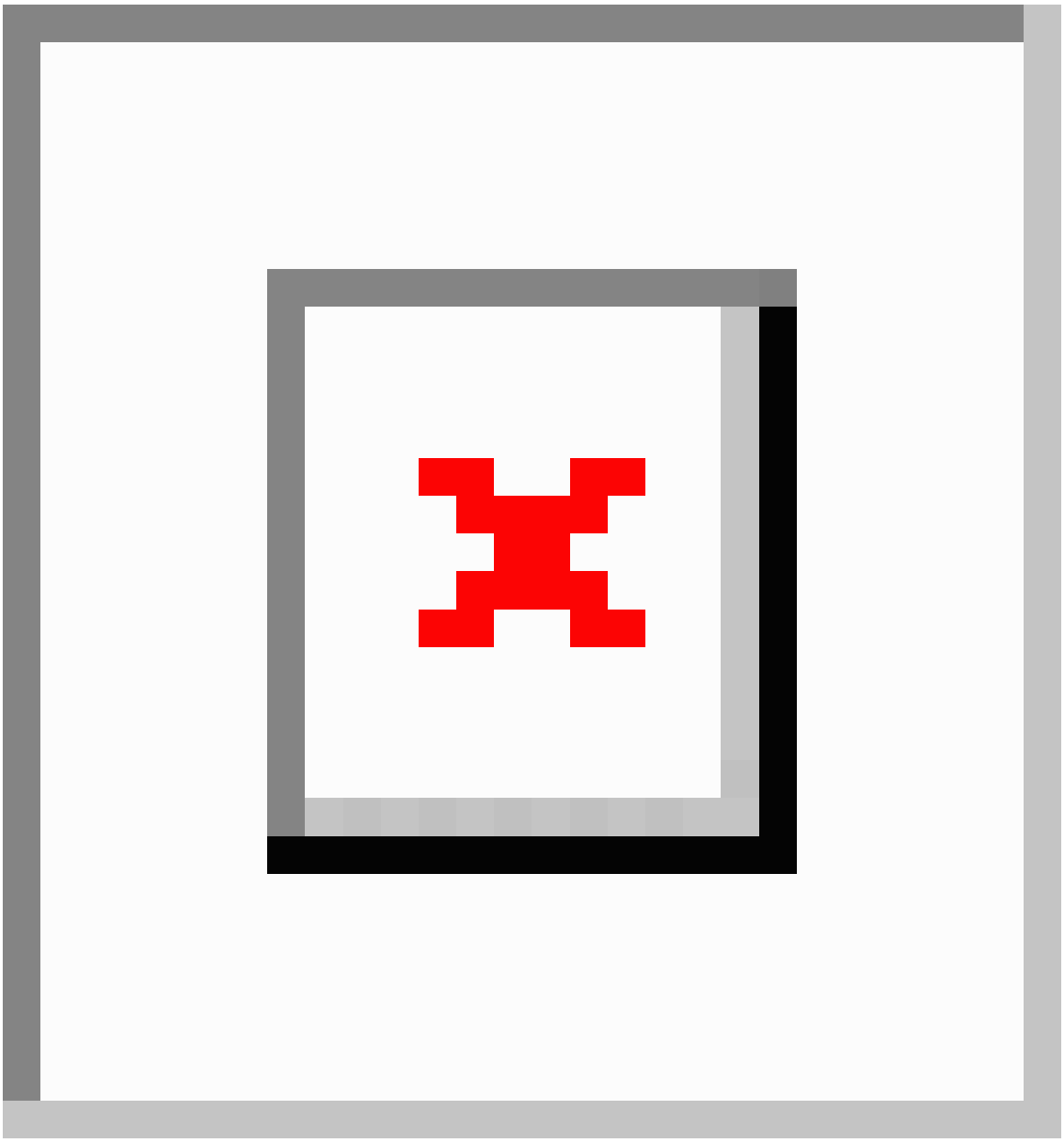
L'exemple suivant montre 2 membres de la grappe dans chacun des 2 centres de données placés entre les routeurs internes et externes (insertion nord-sud). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs locaux en utilisant des EtherChannels étendus pour l'intérieur et l'extérieur. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Les routeurs internes et externes de chaque centre de données utilisent le protocole OSPF, qui est transmis par les périphériques ASA transparents. Contrairement aux MAC, les adresses IP des routeurs sont uniques sur tous les routeurs. En attribuant un routage à coût plus élevé sur l'interface DCI, le trafic reste dans chaque centre de données, sauf si tous les membres de la grappe d'un site donné tombent en panne. La voie de routage

la moins dispendieuse qui traverse les ASA doit traverser le même groupe de ponts sur chaque site pour que la grappe puisse maintenir des connexions dissymétriques. En cas de défaillance de tous les membres de la grappe sur un site, le trafic passe de chaque routeur sur l'interface DCI aux membres de la grappe sur l'autre site.

La mise en œuvre des commutateurs sur chaque site peut inclure :

- VSS inter-sites, vPC, StackWise ou StackWise Virtual : dans ce scénario, vous installez un commutateur au centre de données 1, et l'autre au centre de données 2. Une option consiste à ce que les nœuds de la grappe de chaque centre de données se connectent uniquement au commutateur local, tandis que le trafic du commutateur redondant traverse le DCI. Dans ce cas, les connexions sont pour la plupart conservées localement à chaque centre de données. Vous pouvez éventuellement connecter chaque nœud aux deux commutateurs de la DCI si la DCI peut gérer le trafic supplémentaire. Dans ce cas, le trafic est réparti entre les centres de données, il est donc essentiel que l'interface DCI soit très robuste.
- Local VSS, vPC, StackWise ou StackWise Virtual sur chaque site : Pour une meilleure redondance des commutateurs, vous pouvez installer 2 paires de commutateurs redondants distincts sur chaque site. Dans ce cas, bien que les nœuds de la grappe aient toujours un EtherChannel étendu avec le châssis du centre de données 1 connecté uniquement aux deux commutateurs locaux et le châssis du centre de données 2 connecté à ces commutateurs locaux, l'EtherChannel étendu est essentiellement « divisé ». Chaque système de commutation local redondant voit l'EtherChannel étendu comme un EtherChannel local au site.

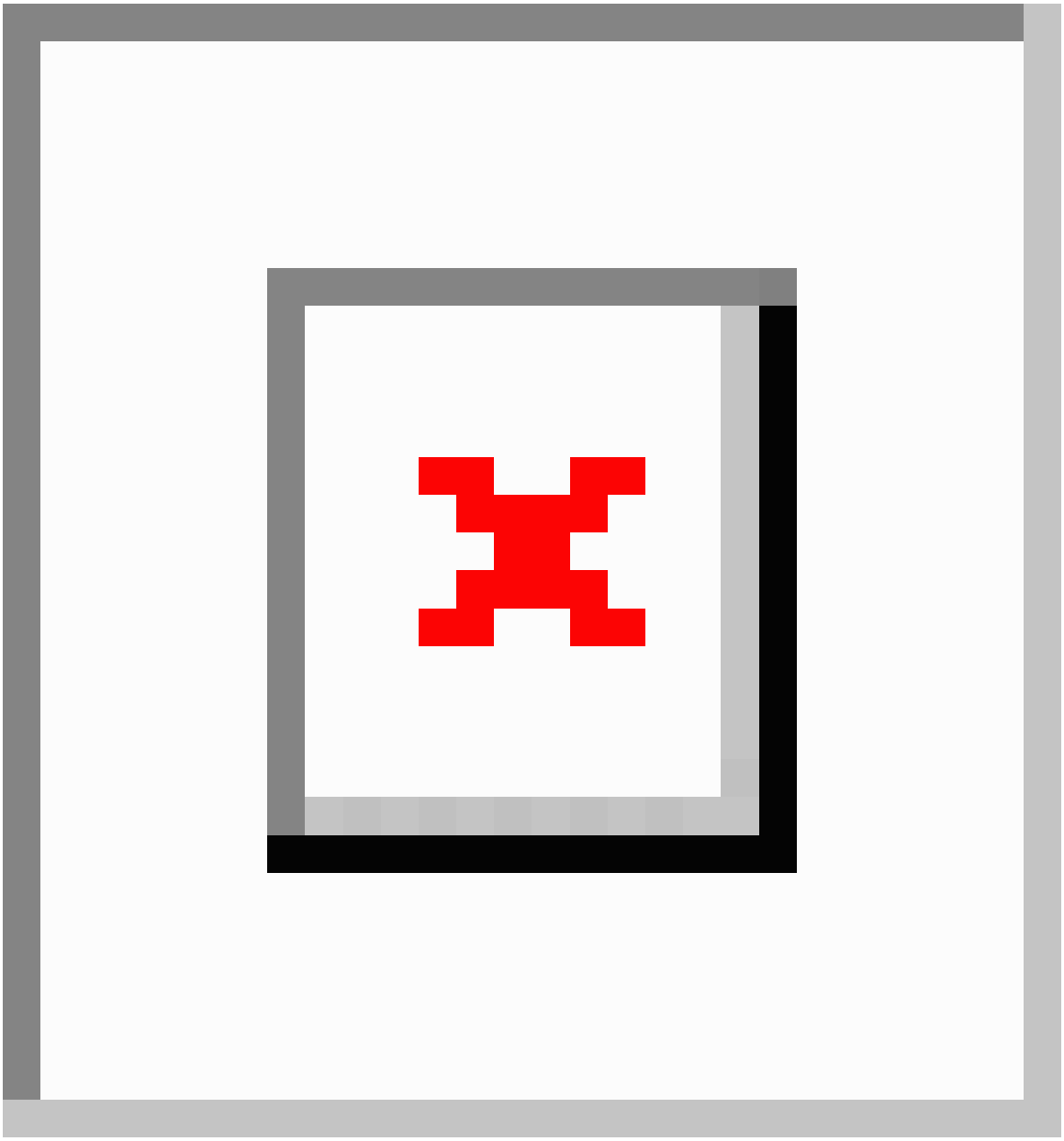


Exemple inter-sites est-ouest en mode transparent de l'EtherChannel étendu

L'exemple suivant montre deux membres de la grappe dans chacun des deux centres de données, placés entre le routeur de la passerelle et deux réseaux internes sur chaque site, le réseau d'applications et le réseau de base de données (insertion est-ouest). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs locaux au moyen d'EtherChannels étendus pour les réseaux App et DB à l'intérieur et à l'extérieur. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Le routeur de la passerelle de chaque site utilise un FHRP comme le HSRP pour fournir les mêmes adresses MAC virtuelles et IP de destination sur chaque site. Une bonne pratique pour éviter le basculement involontaire des adresses MAC consiste à ajouter de manière statique les adresses MAC réelles des routeurs de passerelle

au tableau d'adresses MAC de l'ASA. Sans ces entrées, si la passerelle du site 1 communique avec la passerelle du site 2, ce trafic pourrait passer par l'ASA et tenter d'atteindre le site 2 à partir de l'interface interne, ce qui poserait des problèmes. Les VLAN de données sont étendus entre les sites à l'aide de la virtualisation du transport par superposition (OTV) (ou d'un outil similaire). Vous devez ajouter des filtres pour empêcher le trafic de traverser l'interface DCI vers l'autre site lorsqu'il est destiné au routeur de la passerelle. Si le routeur de la passerelle d'un site devient inaccessible, vous devez supprimer les filtres pour que le trafic puisse être dirigé vers le routeur de la passerelle de l'autre site.



Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités et mise en grappe de l'ASA

Certaines fonctionnalités d'ASA ne sont pas prises en charge avec la mise en grappe d'ASA, et d'autres le sont uniquement sur le nœud de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités non prises en charge par la mise en grappe

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

- Fonctionnalités de communication unifiée qui reposent sur le mandataire TLS
- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Interfaces de tunnel virtuel (VTI)
- Routage IS-IS
- Les inspections d'application suivantes :
  - CTIQBE
  - H323, H225 et RAS
  - Intercommunication IPsec
  - MGCP
  - MMP
  - RTSP
  - SCCP (Skinny)
  - WAAS
  - WCCP
- Filtre de trafic de réseau de zombies
- Auto Update Server
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Équilibrage de la charge VPN
- Basculement
- Routage et pont intégrés
- Détection de connexion inactive (DCD)

- Mode FIPS

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.

Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

- Ces inspections d'application sont prises en charge :
  - DCERPC et ESMTP
  - IM
  - NetBIOS et PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET et SUNRPC
  - TFTP
  - XDMCP
- Surveillance du routage statique
- Autorisation et authentification pour l'accès réseau La comptabilité est décentralisée.
- Services de filtrage
- VPN de site à site

  En mode centralisé, les connexions VPN sont établies avec le nœud de commande de grappe uniquement. Il s'agit du mode par défaut pour la mise en grappe VPN. Le VPN de site à site peut également être déployé en mode VPN distribué, dans lequel les connexions VPN S2S IKEv2 sont réparties sur plusieurs nœuds.
- Traitement du protocole du plan de contrôle de multidiffusion IGMP (le transfert du plan de données est distribué dans la grappe)
- Traitement du protocole du plan de contrôle de multidiffusion PIM (le transfert du plan de données est distribué dans la grappe)

- Routage dynamique

Fonctionnalités appliquées aux unités individuelles

Ces fonctionnalités sont appliquées à chaque nœud ASA, plutôt qu'à la grappe dans son ensemble ou au nœud de contrôle.

- QoS : la politique QoS est synchronisée dans la grappe dans le cadre de la duplication de la configuration. Cependant, la politique est appliquée sur chaque nœud indépendamment. Par exemple, si vous configurez le contrôle en sortie, les valeurs de débit de conformité et de rafale de conformité s'appliquent au trafic sortant d'un ASA particulier. Dans une grappe à 3 nœuds et avec le trafic réparti uniformément, le taux de conformité devient en fait trois fois supérieur au débit de la grappe.
- Détection des menaces : la détection des menaces fonctionne sur chaque nœud indépendamment; par exemple, les statistiques principales sont propres au nœud. La détection de l'analyse de port, par exemple, ne fonctionne pas, car l'analyse du trafic sera équilibrée entre tous les nœuds et un nœud ne verra pas tout le trafic.
- Gestion des ressources : la gestion des ressources en mode contexte multiple est appliquée séparément sur chaque nœud en fonction de l'utilisation locale.
- Trafic LISP : le trafic LISP sur le port UDP 4342 est inspecté par chaque nœud de réception, mais aucun directeur n'est affecté. Chaque nœud ajoute au tableau EID qui est partagé dans la grappe, mais le trafic LISP lui-même ne participe pas au partage de l'état de la grappe.

AAA pour l'accès réseau et la mise en grappe

L'AAA pour l'accès réseau comprend trois composants : l'authentification, l'autorisation et la gestion de comptes. L'authentification et l'autorisation sont mises en œuvre en tant que fonctionnalités centralisées sur le nœud de contrôle de mise en grappe avec la duplication des structures de données sur les nœuds de données de grappe. Si un nœud de contrôle est choisi, le nouveau nœud de contrôle disposera de toute l'information nécessaire pour continuer le fonctionnement ininterrompu des utilisateurs authentifiés établis et de leurs autorisations associées. Les délais d'inactivité et absolus pour l'authentification des utilisateurs sont conservés lorsqu'un changement de nœud de contrôle se produit.

La comptabilité est mise en œuvre en tant que fonctionnalité distribuée dans une grappe. La comptabilité est effectuée flux par flux, de sorte que le nœud de la grappe possédant un flux enverra les messages de démarrage et d'arrêt de comptabilité au serveur AAA lorsque la comptabilité est configurée pour un flux.

Paramètres de connexion

Les limites de connexion s'appliquent à l'ensemble de la grappe (voir **Configuration** > **Firewall** > **Service Policy**, page). Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le

propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.

- Si vous utilisez l'AAA pour l'accès FTP, le flux du canal de contrôle est centralisé sur le nœud de contrôle.

Inspection ICMP

Le flux des paquets d'erreurs ICMP et ICMP dans la grappe varie selon que l'inspection d'erreurs ICMP ou ICMP est activée ou non. Sans inspection ICMP, ICMP est un flux unidirectionnel et il n'y a pas de prise en charge de flux directeur. Avec l'inspection ICMP, le flux ICMP devient bidirectionnel et est soutenu par un flux directeur/de sauvegarde. L'une des différences avec un flux ICMP inspecté réside dans le traitement par le directeur du paquet transféré : le directeur transmettra le paquet de réponse d'écho ICMP au propriétaire du flux au lieu de retourner le paquet au transitaire.

Routage multidiffusion et mise en grappe

L'unité de contrôle gère tous les paquets de routage de multidiffusion et les paquets de données jusqu'à ce que le transfert rapide soit établi. Une fois la connexion établie, chaque unité de données peut transférer des paquets de données en multidiffusion.

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents ASAdans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à ASA qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :
  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.
  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraîneront des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouvel ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.
  - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer

toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.

- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, la grappe divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.
- Réutiliser un pool PAT dans plusieurs règles : pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interfaces dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.
- Pas de tourniquet : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.
- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.
- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.
- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.
- Fonctionnalité PAT par session : bien qu'elle ne soit pas exclusive à la mise en grappe, la fonctionnalité PAT par session améliore l'évolutivité de PAT et, pour la mise en grappe, permet à chaque nœud de données de posséder des connexions PAT; en revanche, les connexions PAT multisessions doivent être transférées au nœud de contrôle et détenues par celui-ci. Par défaut, tout le trafic TCP et le trafic DNS UDP utilisent un xlate PAT par session, tandis que ICMP et tout le reste du trafic UDP utilise la multisession. Vous pouvez configurer des règles NAT par session pour modifier ces valeurs par défaut pour TCP et UDP, mais vous ne pouvez pas configurer la PAT par session pour ICMP. Par exemple, en raison de l'utilisation croissante du protocole Quic sur le port UDP/443 comme alternative de performance à HTTPS TLS sur TCP/443, vous devriez activer la traduction d'adresses par session (PAT) pour UDP/443. Pour le trafic qui bénéficie de la PAT multisession, comme le H.323, le SIP ou l'interface simplifiée, vous pouvez désactiver la PAT par session pour les ports TCP associés (les ports UDP de ces ports H.323 et SIP sont déjà multisession en par défaut). Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.
- Pas de PAT statique pour les inspections suivantes :
  - FTP
  - PPTP
  - RSH

- SQLNET
- TFTP
- XDMCP
- SIP

- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

Lignes directrices pour la NAT et la mise en grappe

Passez en revue ces lignes directrices relatives à la NAT et à la mise en grappe :

Lignes directrices générales

- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, la grappe divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.
- Réutiliser un pool PAT dans plusieurs règles : pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interfaces dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.
- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.
- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

Limites relatives à la NAT et à la mise en grappe

Passez en revue ces limites relatives à la NAT et à la mise en grappe :

Restrictions générales

- Pas de PAT statique pour les inspections suivantes :

- FTP
- PPTP
- RSH
- SQLNET
- TFTP
- XDMCP
- SIP

- Pas de tourniquet : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.
- La PAT étendue n'est pas prise en charge avec la mise en grappe.
- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.

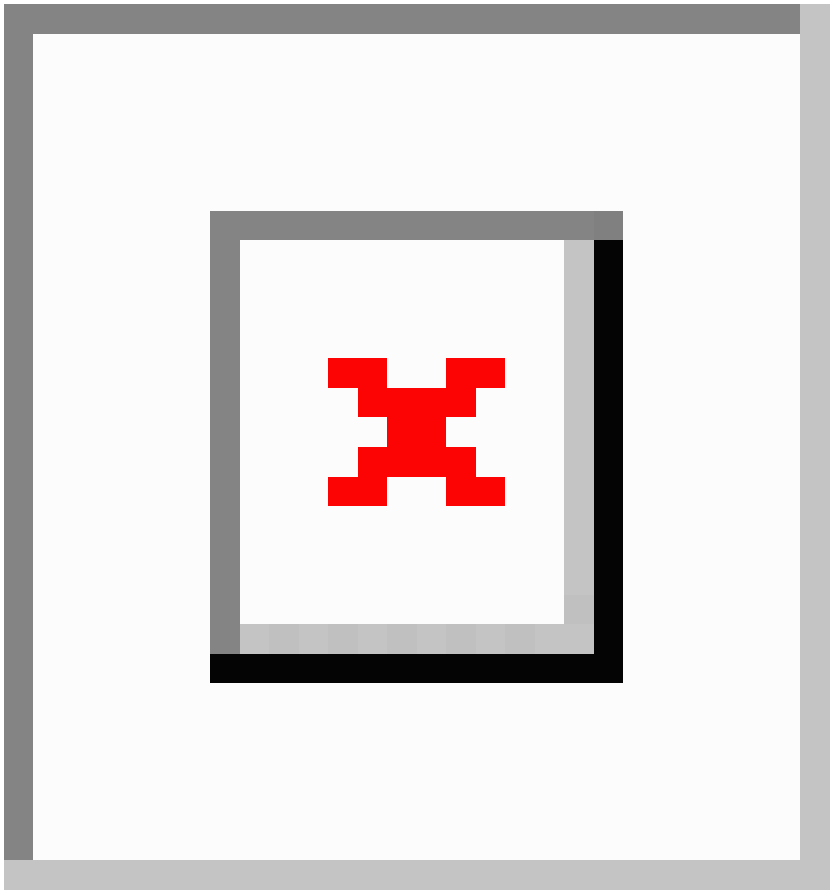
PAT avec limites d'allocation de bloc de port

- La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
- Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.
- Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraîneront des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouvel ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.
- Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.

Routage et mise en grappe dynamiques

Le processus de routage ne s'exécute que sur l'unité de contrôle, et les routages sont appris par l'unité de contrôle et répliqués sur les serveurs secondaires. Si un paquet de routage arrive à une unité de données, il est redirigé vers l'unité de contrôle.

Illustration 62 : Routage dynamique



Une fois que les unités de données ont appris les routages de l'unité de contrôle, chaque unité prend les décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée entre l'unité de contrôle et les unités de données. S'il y a un basculement de l'unité de contrôle, le routeur voisin détectera un redémarrage; le basculement n'est pas transparent. Le processus OSPF choisit une adresse IP comme ID de routeur. Bien que cela ne soit pas obligatoire, vous pouvez attribuer un ID de routeur statique pour vous assurer qu'un ID de routeur cohérent est utilisé dans la grappe. Consultez la fonctionnalité de transfert sans arrêt OSPF pour gérer l'interruption.

SCTP et mise en grappe

Une association SCTP peut être créée sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses connexions multi-hébergement doivent résider sur le même nœud.

Inspection SIP et mise en grappe

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

La configuration du mandataire TLS n'est pas prise en charge.

SNMP et mise en grappe

Un agent SNMP interroge chaque ASA en fonction de l'adresse IP locale de son . Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud.Vous devez les rajouter sur le nœud de contrôle pour forcer les utilisateurs à se reproduire vers le nouveau nœud, ou directement sur le nœud de données.

STUN et mise en grappe

L'inspection STUN est prise en charge dans les modes de basculement et de grappe, car les sténopés sont dupliqués. Cependant, l'ID de transaction n'est pas répliqué sur les nœuds. Dans le cas où un nœud tombe en panne après avoir reçu une demande STUN et qu'un autre nœud a reçu la réponse STUN, la réponse STUN sera abandonnée.

Syslog, NetFlow et la mise en grappe

- Syslog : chaque nœud de la grappe génère ses propres messages de journal système. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.
- NetFlow : chaque nœud de la grappe génère son propre flux NetFlow. Le collecteur NetFlow peut traiter chaque appareil ASA uniquement comme un exportateur NetFlow distinct.

Cisco TrustSec et la mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

VPN et mise en grappe sur le châssis Secure Firewall eXtensible Operating System (FXOS)

Une grappe ASA FXOS prend en charge l'un des deux modes mutuellement exclusifs pour le VPN de S2S, centralisé ou distribué :

- Mode VPN centralisé. Le mode par défaut. En mode centralisé, les connexions VPN sont établies avec l'unité de commande de grappe uniquement.

  La fonctionnalité VPN est limitée à l'unité de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si l'unité de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues et les utilisateurs connectés au VPN subissent une interruption de service. Lorsqu'une nouvelle unité de contrôle est choisie, vous devez rétablir les connexions VPN.

Lorsque vous connectez un tunnel VPN à une adresse d'interface étendue, les connexions sont automatiquement transférées à l'unité de contrôle. Les clés et les certificats VPN sont répliqués sur toutes les unités.

- Mode de VPN distribué. Dans ce mode, les connexions VPN S2S IPsec IKEv2 sont réparties sur les membres d'une grappe ASA, ce qui offre une grande évolutivité. La distribution des connexions VPN entre les membres d'une grappe permet d'utiliser pleinement la capacité et le débit de la grappe, ce qui augmente considérablement la prise en charge des VPN au-delà des capacités VPN centralisées.

Remarque

Le mode de mise en grappe VPN centralisée prend en charge S2S IKEv1 et S2S IKEv2.

Le mode de mise en grappe du VPN distribué prend uniquement en charge S2S, IKEv2.

Le mode de mise en grappe du VPN distribué est pris en charge sur le Firepower 9300 uniquement.

Le VPN d'accès à distance n'est pas pris en charge en mode de mise en grappe de VPN centralisé ou distribué.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Par exemple, pour le débit TCP, le périphérique Firepower 9300 avec ses 3 modules SM-40 peut gérer environ 135 Gbit/s du trafic de pare-feu du monde réel lorsqu'il fonctionne seul. Pour le double châssis, le débit maximal combiné sera d'environ 80 % des 270 Gbit/s (2 châssis x 135 Gbit/s) : 216 Gbit/s.

Choix d'unité de contrôle

Les membres de la grappe communiquent sur le lien de commande de grappe pour élire une unité de contrôle comme suit :

1. Lorsque vous déployez la grappe, chaque unité diffuse une demande de sélection toutes les 3 secondes.
2. toute autre unité ayant un niveau de priorité plus élevée répondra à la demande de sélection; la priorité est définie lorsque vous déployez la grappe et n'est pas configurable.
3. Si, après 45 secondes, une unité ne reçoit pas de réponse d'une autre unité de priorité plus élevée, elle devient l'unité de contrôle.

Remarque

Si plusieurs unités sont à égalité pour la priorité la plus élevée, le nom de l'unité de la grappe suivi du numéro de série est utilisé pour déterminer l'unité de contrôle.

4. Si une unité se joint ultérieurement à la grappe avec une priorité plus élevée, elle ne devient pas automatiquement l'unité de contrôle; l'unité de contrôle existante conserve toujours ses fonctions d'unité de contrôle, sauf si elle arrête de répondre, auquel cas une nouvelle unité de contrôle est élue.
5. Dans un scénario de « split-brain » (processeur partagé), où il y a temporairement plusieurs unités de contrôle, l'unité ayant la priorité la plus élevée conserve le rôle tandis que les autres unités retournent aux rôles d'unité de données.

Remarque Vous pouvez forcer manuellement une unité à devenir l'unité de contrôle. Pour les fonctions centralisées, si vous forcez le changement d'unité de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur la nouvelle unité de contrôle.

Haute disponibilité au sein de la grappe

La mise en grappe assure une disponibilité élevée en surveillant l'intégrité du châssis, des unités et de l'interface, et en reproduisant les états de connexion entre les unités.

Surveillance des applications du châssis

La surveillance de l'intégrité de l'application du châssis est toujours activée. Le superviseur Châssis Firepower 4100/9300 vérifie l'application ASA régulièrement (à chaque seconde). Si l'ASA est opérationnel et ne peut pas communiquer avec le superviseur Châssis Firepower 4100/9300 pendant 3 secondes, l'ASA génère un message syslog et quitte la grappe.

Si le superviseur Châssis Firepower 4100/9300 ne peut pas communiquer avec l'application après 45 secondes, il recharge l'ASA. Si l'ASA ne peut pas communiquer avec le superviseur, il se supprime de la grappe.

Surveillance de l'intégrité de l'unité

Chaque unité envoie périodiquement un paquet de diffusion keepaliveheartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet keepaliveheartbeat ou autre paquet d'un nœud de données au cours de la période d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est choisi parmi le nœud restant.

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle. Consultez Choix d'unité de contrôle, à la page 527 pour de plus amples renseignements.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles utilisées et signale les modifications d'état au nœud de contrôle. Pour la mise en grappe sur plusieurs châssis, les EtherChannels étendus utilisent le protocole cLACP (Link Aggregation Control Protocol). Chaque châssis surveille l'état de la liaison et les messages du protocole cLACP pour déterminer si le port est toujours actif dans l'EtherChannel et informe l'application ASA si l'interface est en panne. Lorsque vous activez la surveillance de l'intégrité, les interfaces physiques sont surveillées par défaut (y compris l'interface principale EtherChannel pour les interfaces EtherChannel). Seules les interfaces nommées qui sont dans un état activé peuvent être surveillées. Par exemple, tous les ports membres d'un EtherChannel doivent tomber en panne avant qu'un EtherChannel *nommé* ne soit supprimé de la grappe (selon votre paramètre de regroupement de ports minimal). Vous pouvez éventuellement désactiver la surveillance par interface.

Si une interface surveillée tombe en panne sur un nœud particulier, mais qu'elle est active sur d'autres nœuds, ce nœud est supprimé de la grappe. Le délai avant la suppression par ASA d'un nœud de la grappe dépend du fait que le nœud est un membre établi ou qu'il rejoint la grappe. L'ASA ne surveille pas les interfaces pendant les 90 premières secondes où un nœud rejoint la grappe. Les changements d'état de l'interface pendant cette période n'entraîneront pas le retrait de l'ASA de la grappe. Pour un membre établi, le nœud est supprimé après 500 ms.

Pour la mise en grappe sur plusieurs châssis, si vous ajoutez ou supprimez un EtherChannel de la grappe, la surveillance de l'intégrité de l'interface est suspendue pendant 95 secondes pour que vous ayez le temps d'effectuer les modifications sur chaque châssis.

Surveillance de l'application Decorator

Lorsque vous installez une application décorateur sur une interface, comme l'application Radware DefensePro, ASA et l'application décorateur doivent être opérationnels pour rester dans la grappe. L'unité ne rejoint pas la grappe tant que les deux applications ne sont pas opérationnelles. Une fois dans la grappe, l'unité surveille l'intégrité de l'application du séparateur toutes les 3 secondes. Si l'application décorateur est en panne, l'unité est supprimée de la grappe.

État après l'échec

Lorsqu'un nœud de la grappe tombe en panne, les connexions hébergées par ce nœud sont transférées en toute transparence vers d'autres nœuds; Les renseignements d'état sur les flux de trafic sont partagés sur la liaison de commande de grappe du nœud de contrôle.

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

ASA tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.

Remarque Lorsque ASA devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe, l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Rejoindre la grappe

Après le retrait d'un membre de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : l'ASA essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment. Ce comportement est configurable.
- Échec de l'interface de données : l'ASA tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'ASA désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe.Ce comportement est configurable.

- Unité en échec : si l'unité a été supprimée de la grappe en raison d'un échec de vérification de l'intégrité de l'unité, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que l'unité rejoindra la grappe au redémarrage, à condition que la liaison de commande de grappe soit active. L'unité tente de rejoindre la grappe toutes les 5 secondes.
- Échec de la communication Châssis-Application : lorsque l'ASA détecte que l'intégrité de l'application de châssis a été récupérée, l'ASA essaie de rejoindre la grappe immédiatement.
- Échec de l'application de décorateur : l'ASA rejoint la grappe lorsqu'il détecte que l'application de décorateur est sauvegardée.
- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc. Une unité tentera de rejoindre la grappe automatiquement aux intervalles suivants : 5 minutes, 10 minutes, puis 20 minutes. Ce comportement est configurable.

Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 23 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
Tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	Comprend les règles AAA (uauth).
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—
VPN distribué (site à site) pour Firepower 4100/9300	Oui	La session de sauvegarde devient la session active, puis une nouvelle session de sauvegarde est créée.

Gestion des connexions par la grappe

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.
- Propriétaire de la sauvegarde : nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

  Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis.

  Si vous activez la localisation du directeur pour la mise en grappe inter-sites, il existe deux rôles de propriétaire de la sauvegarde : le rôle de sauvegarde locale et de sauvegarde globale. Le propriétaire choisit toujours une sauvegarde locale sur le même site que lui (en fonction de l'ID du site). La sauvegarde globale peut se trouver sur n'importe quel site et peut même se trouver sur le même nœud que la sauvegarde locale. Le propriétaire envoie des informations sur l'état de la connexion aux deux sauvegardes.

  Si vous activez la redondance de sites et que le propriétaire de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La sauvegarde de châssis et la sauvegarde de site sont indépendantes. Par conséquent, dans certains cas, un flux comportera à la fois une sauvegarde de châssis et une sauvegarde de site.
- Directeur : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

  Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Si vous activez la localisation de directeur pour la mise en grappe inter-sites, il y a deux rôles de directeur : le directeur local et le directeur global. Pour un paquet de nouveau flux, le membre de réception sélectionne le directeur local parmi les membres du site du membre de réception. Le directeur global peut se trouver sur n'importe quel site et peut même être le même membre que le directeur local. En cas de défaillance du propriétaire d'origine et lorsque la localisation s'applique, le directeur local choisit un nouveau propriétaire de connexion sur le site du directeur local.

Détails du hachage ICMP/ICMPv6 :

- Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
- Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
- Pour les autres paquets, les ports source et de destination sont à 0.

- Transitaire : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Si vous activez la localisation de directeur, le redirecteur interroge le directeur local lorsque la localisation s'applique. Le transitaire interroge le directeur global si le directeur local ne connaît pas le propriétaire, si la connexion appartient à un autre site ou si la localisation est contournée. Une requête de directeur intersite est le comportement attendu dans ces cas. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.

Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

- Propriétaire de fragment : pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

Connexions par traduction d'adresse de port

Lorsqu'une connexion utilise la traduction d'adresses de port (PAT), le type de PAT (par session ou multisession) influence quel membre de la grappe devient propriétaire de la nouvelle connexion :

- PAT par session : le propriétaire est le nœud qui reçoit le paquet initial dans la connexion.

  Par défaut, le trafic TCP et DNS UDP utilise une PAT par session.

- PAT multisession : le propriétaire est toujours le nœud de contrôle. Si une connexion PAT multisession est initialement reçue par un nœud de données, le nœud de données transfère la connexion au nœud de contrôle.

  Par défaut, le trafic UDP (à l'exception du trafic UDP DNS) et ICMP utilise la PAT multisession. Ces connexions appartiennent donc toujours au nœud de contrôle.

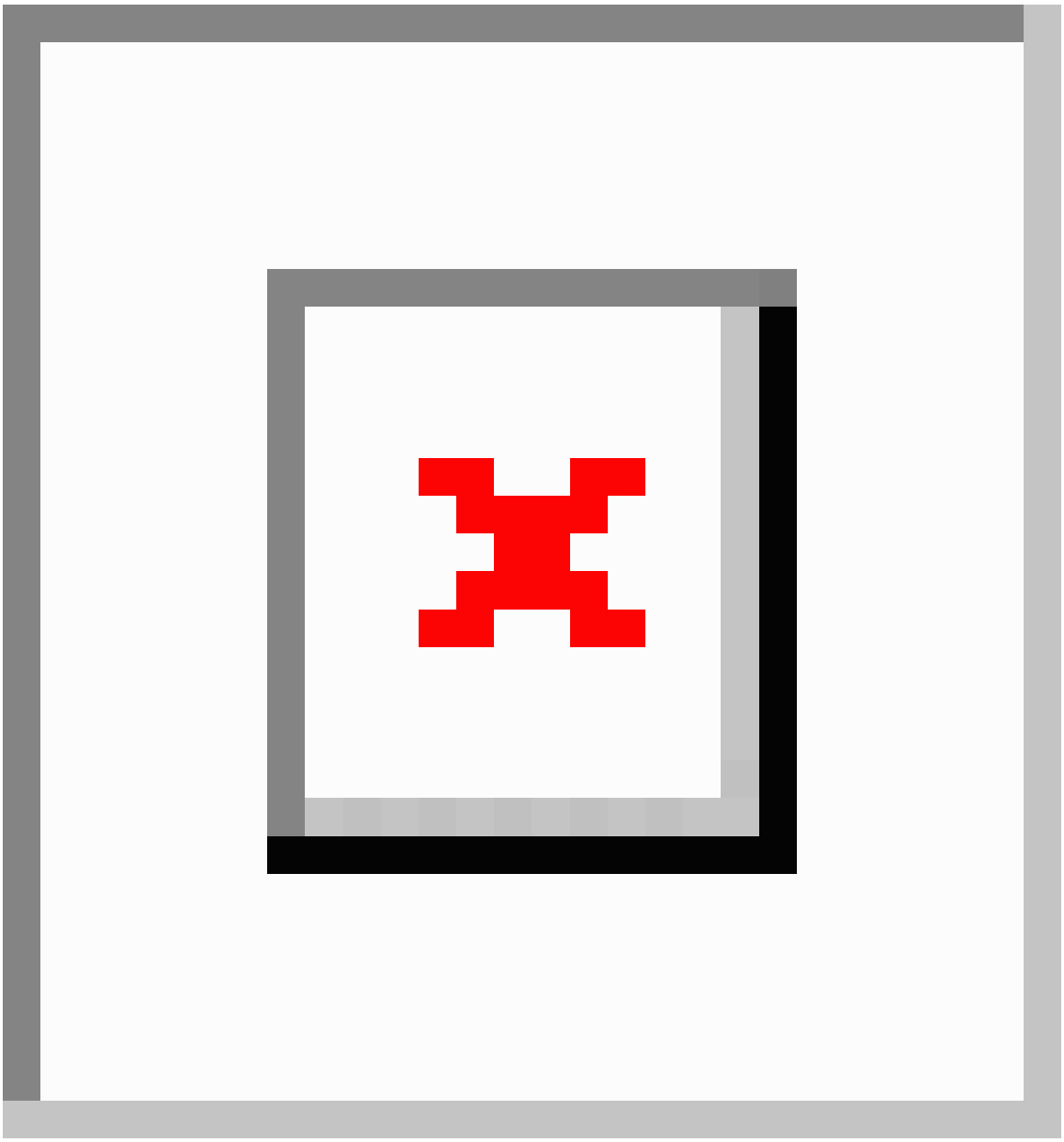
Vous pouvez modifier les valeurs par défaut de PAT par session pour les protocoles TCP et UDP afin que les connexions à ces protocoles soient gérées par session ou multisession selon la configuration. Pour ICMP, vous ne pouvez pas modifier la PAT multisession par défaut. Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.



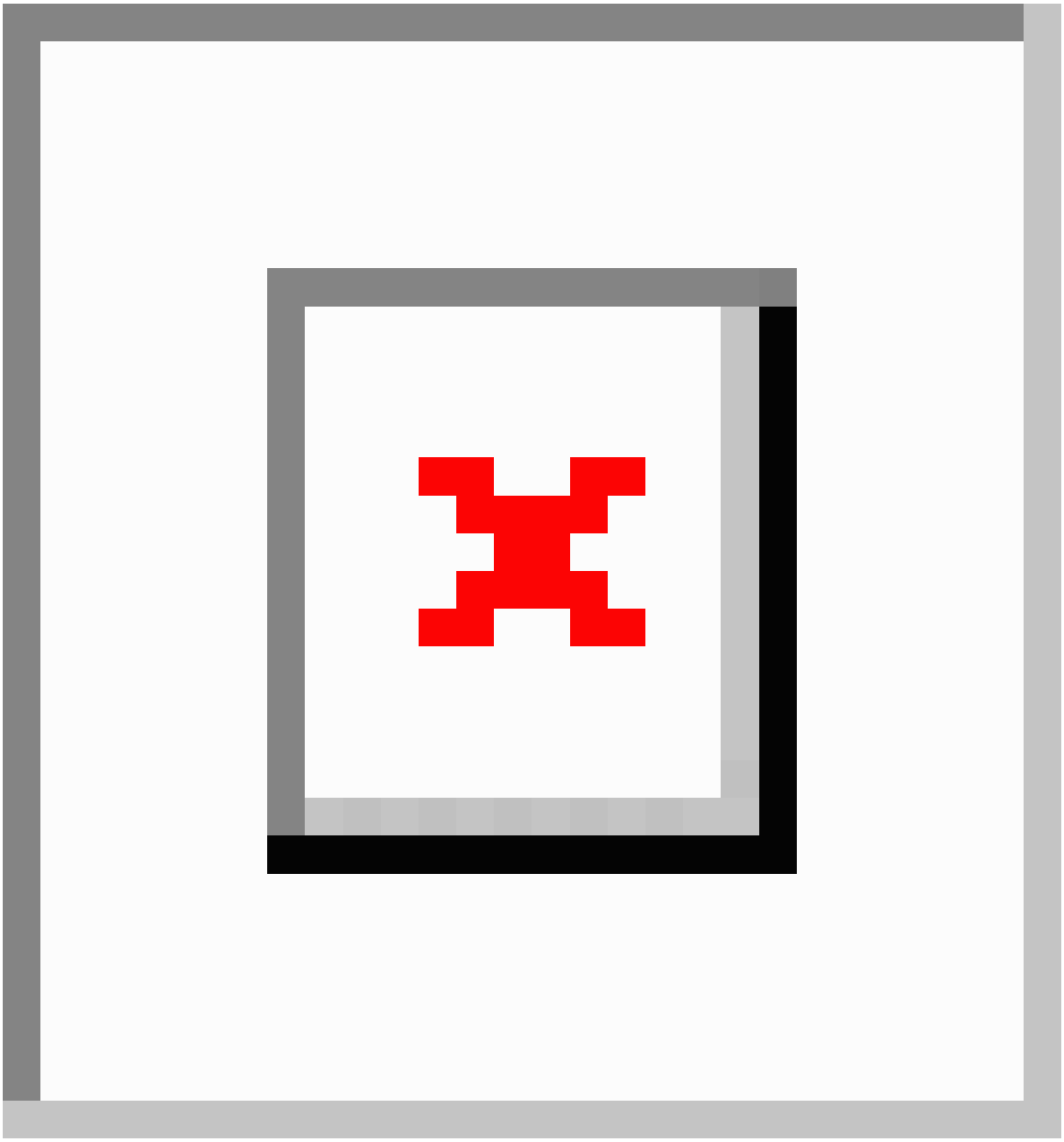
1. Le paquet SYN provient du client et est livré à un ASA (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un ASA différent (selon la méthode d'équilibrage de la charge). Cet ASA est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.

5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.
7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. *Illustration 63 : Flux de données ICMP et UDP*



Le premier paquet UDP provient du client et est remis à un ASA (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.

6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.
8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Rééquilibrage des nouvelles connexions TCP dans la grappe

Si les capacités d'équilibrage de charges des routeurs en amont ou en aval entraînent une répartition non équilibrée des flux, vous pouvez configurer un rééquilibrage des nouvelles connexions afin que les nœuds ayant le plus de nouvelles connexions par seconde redirigent les nouveaux flux TCP vers d'autres nœuds. Aucun flux existant ne sera déplacé vers d'autres nœuds.

Comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal.

Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

Historique de la mise en grappe d'ASA sur le Firepower 4100/9300

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Suppression des propos tendancieux	9.19(1)	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Amélioration de l'attribution des blocs de ports PAT pour la mise en grappe sur le Firepower 4100/9300	9.16(1)	L'allocation améliorée des blocs de ports PAT garantit que l'unité de contrôle conserve des ports en réserve pour les nœuds en cours de jonction et récupère de manière proactive les ports inutilisés. Pour optimiser au mieux l'allocation, vous pouvez définir le nombre maximum de nœuds que vous prévoyez d'avoir dans la grappe à l'aide de la commande **cluster-member-limit**. L'unité de contrôle peut ensuite allouer des blocs de ports au nombre de nœuds planifié sans avoir à réserver des ports pour des nœuds supplémentaires que vous ne comptez pas utiliser. La valeur par défaut est de 16 nœuds. Vous pouvez également surveiller le journal système 747046 pour vous assurer qu'il y a suffisamment de ports disponibles pour un nouveau nœud. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)** > **Cluster Member Limit (Limite de membres de la grappe)** champ
Améliorations de la commande **show cluster history**	9.16(1)	Nous avons ajouté des sorties supplémentaires pour la commande **show cluster history**. Commandes nouvelles ou modifiées : **show cluster history brief**, **show cluster history latest**, **show cluster history reverse**, **show cluster history time**
Test de ping MTU depuis le nœud de contrôle lors de la jonction d'un nœud	9.16(1)	Lorsqu'un nœud rejoint la grappe, le nœud de contrôle vérifie la compatibilité de la MTU en envoyant un ping au nœud de données avec une taille de paquet deux fois supérieure à la MTU de la liaison de commande de la grappe. Si l'envoi du message Ping échoue, une notification est générée afin que vous puissiez corriger l'incompatibilité MTU sur les commutateurs de connexion et réessayer. Écrans ajoutés/modifiés : **Monitoring (Surveillance)** > **ASA Cluster (Grappe ASA)** > **Cluster Summary (Résumé de la grappe)**
Synchronisation de la configuration avec les unités de données en parallèle	9.14(1)	L'unité de contrôle synchronise maintenant les changements de configuration avec les unités de données en parallèle par défaut. Auparavant, la synchronisation se produisait de manière séquence. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)** > **case Enable parallel configuration replicate (Activer la réplication de configuration parallèle)**
Messages pour un échec de jonction de grappe ou une éviction ajoutés à **show cluster history**	9.14(1)	De nouveaux messages ont été ajoutés à la commande **show cluster history** lorsqu'une unité de grappe ne parvient pas à rejoindre la grappe ou la quitter. Commandes nouvelles ou modifiées : **show cluster history** Nouveaux écrans ou modifiés : aucun.
Informations sur l'initiateur et le répondeur pour la détection des connexions inactives (DCD) et prise en charge du DCD dans une grappe.	9.13(1)	Si vous activez la détection des connexions inactives (DCD), vous pouvez utiliser la commande **show conn detail** pour obtenir des informations sur l'initiateur et le répondeur. La détection des connexions inactives vous permet de maintenir une connexion inactive, et la sortie **show conn** vous indique la fréquence à laquelle les points terminaux ont été sondés. En outre, DCD est désormais pris en charge dans une grappe. Aucun écran modifié.

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Superviser la charge de trafic pour une grappe	9.13(1)	Vous pouvez désormais superviser la charge de trafic pour les membres de la grappe, y compris le nombre total de connexions, l'utilisation du CPU et de la mémoire, ainsi que les abandons de tampon. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur l'unité si les unités restantes peuvent gérer la charge ou de régler l'équilibrage de charges sur le commutateur externe. Cette fonction est activée par défaut. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)** > **case Enable Cluster Load Monitor (Activer le moniteur de charge de la grappe)** • **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Load-Monitoring (Supervision de la charge de la grappe)**
Jonction de grappe accélérée	9.13(1)	Lorsqu'une unité de données a la même configuration que l'unité de contrôle, elle ignorera la synchronisation de la configuration et se joindra plus rapidement. Cette fonction est activée par défaut. Cette fonctionnalité est configurée sur chaque unité et n'est pas répliquée de l'unité de contrôle à l'unité de données. **Remarque** Certaines commandes de configuration ne sont pas compatibles avec la jonction accélérée de grappes; si ces commandes sont présentes sur l'unité, même si la jonction accélérée de grappes est activée, la synchronisation de la configuration se produira toujours. Vous devez supprimer la configuration incompatible pour que la jonction accélérée de grappes fonctionne. Utilisez la commande **show cluster info unit-join-acceleration incompatible-config** pour afficher la configuration incompatible. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)** > **case Enable config sync acceleration (Activer l'accélération de la synchronisation de la configuration)**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Protocole ARP gratuit par site pour la mise en grappe	9.12(1)	L'ASA génère maintenant des paquets ARP gratuits (GARP) pour maintenir l'infrastructure de commutation à jour : le membre ayant la priorité la plus élevée sur chaque site génère périodiquement du trafic GARP pour les adresses MAC et IP globales. Lorsque vous utilisez des adresses MAC et IP par site, les paquets provant de la grappe utilisent une adresse MAC et une adresse IP propres au site, tandis que les paquets reçus par la grappe utilisent une adresse MAC et une adresse IP globales. Si le trafic n'est pas généré périodiquement à partir de l'adresse MAC globale, vous pourriez rencontrer un délai d'expiration de l'adresse MAC sur vos commutateurs pour l'adresse MAC globale. Après un délai d'expiration, le trafic destiné à l'adresse MAC globale sera inondé dans l'ensemble de l'infrastructure de commutation, ce qui peut entraîner des problèmes de performance et de sécurité. Le GARP est activé par défaut lorsque vous définissez l'ID de site pour chaque unité et l'adresse MAC du site pour chaque EtherChannel étendu. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)** > **Site Periodic GARP (GARP périodique du site)** champ
Groupement d'unités de grappe en parallèle par châssis Firepower 9300	9.10(1)	Pour Firepower 9300, cette fonctionnalité garantit que les modules de sécurité d'un châssis rejoignent la grappe simultanément afin que le trafic soit réparti uniformément entre les modules. Si un module se joint très avant les autres modules, il peut recevoir plus de trafic que souhaité, car les autres modules ne peuvent pas encore partager la charge. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** Options nouvelles ou modifiées : zone **Parallel Join of Units Per Chassis**
Adresse IP personnalisable par liaison de commande de grappe pour le Firepower 4100/9300	9.10(1)	Par défaut, la liaison de commande de grappe utilise le réseau 127.2.0.0/16. Vous pouvez maintenant définir le réseau lorsque vous déployez la grappe dans FXOS. Le châssis génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID du châssis et de l'ID d'emplacement : 127.2.*chassis_id*.*slot_id*. Cependant, certains déploiements réseau ne permettent pas le passage du trafic 127.2.0.0/16. Par conséquent, vous pouvez maintenant définir un sous-réseau personnalisé /16 pour la liaison de commande de grappe dans FXOS, à l'exception des adresses de boucle avec retour (127.0.0.0/8) et de multidiffusion (224.0.0.0/4). Écrans Nouveaux ou modifiés de Firewall Chassis Manager : **Logical Devices (Dispositifs logiques)** > **Add Device (Ajouter un périphérique)** > **Cluster Information (Renseignements relatifs à la grappe)** Options nouvelles ou modifiées : champ **CCL Subnet IP**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Le délai de réponse de l'interface de grappe s'applique désormais aux interfaces qui passent d'un état inactif à un état opérationnel.	9.10(1)	Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié dans la commande **health-check monitor-interface debounce-time** ou dans l'écran **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** d'ASDM avant de marquer l'interface comme ayant échoué et que l'unité soit supprimée de la grappe. Cette fonctionnalité s'applique désormais aux interfaces qui passent d'un état inactif à un état opérationnel. Par exemple, dans le cas d'un EtherChannel qui passe d'un état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un délai de réponse plus long peut empêcher l'interface de sembler être défaillante sur une unité de la grappe juste parce qu'une autre unité de la grappe a été plus rapide à regrouper les ports. Nous n'avons pas modifié d'écrans.
Rejoindre automatiquement la grappe après une défaillance interne	9.9(2)	Auparavant, de nombreuses conditions d'erreur entraînaient le retrait d'une unité de la grappe et vous deviez rejoindre manuellement la grappe après avoir résolu le problème. Désormais, une unité tentera de rejoindre la grappe automatiquement aux intervalles suivants par défaut : 5 minutes, 10 minutes, puis 20 minutes. Ces valeurs sont configurables. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Auto Rejoin (Jonction automatique)**
Afficher les statistiques relatives au transport pour les messages du protocole de transport fiable de la grappe	9.9(2)	Vous pouvez désormais afficher l'utilisation du tampon de transport fiable par grappe d'unités afin de cerner les problèmes d'abandon de paquet lorsque le tampon est plein dans le plan de commande. Commande nouvelle ou modifiée : **show cluster info transport cp detail**
Le comportement de la commande **cluster remove unit** correspond au comportement **no enable**	9.9(1)	La commande **cluster remove unit** supprime maintenant une unité de la grappe jusqu'à ce que vous réactiviez manuellement la mise en grappe ou la rechargiez, de manière similaire à la commande **no enable**. Auparavant, si vous redéployiez la configuration de démarrage à partir de FXOS, la mise en grappe était réactivée. Désormais, l'état désactivé persiste même dans le cas d'un redéploiement de la configuration de démarrage. Cependant, le rechargement de l'ASA réactivera la mise en grappe. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**
Amélioration de la détection des échecs de vérification de l'intégrité du châssis	9.9(1)	Vous pouvez désormais configurer un délai de rétention inférieur pour la vérification de l'intégrité du châssis : 100 ms. Le minimum précédent était de 300 ms. Notez que la durée minimum combinée (*intervalle* x *nombre de tentatives*) ne peut pas être inférieure à 600 ms. Commande nouvelle ou modifiée : **app-agent heartbeat interval** ASDM n'est pas pris en charge.

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Redondance inter-sites pour la mise en grappe	9.9(1)	La redondance inter-sites garantit qu'un propriétaire de secours pour un flux de trafic se trouvera toujours sur l'autre site que le propriétaire. Cette fonctionnalité offre une protection contre les défaillances du site. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**
VPN de site à site distribué avec mise en grappe sur le Firewall 9300	9.9(1)	Une grappe ASA sur le Firewall 9300 prend en charge le VPN de site à site en mode distribué. Le mode distribué permet d'avoir de nombreuses connexions VPN IPsec IKEv2 de site à site réparties sur les membres d'une grappe ASA, pas seulement sur l'unité de contrôle (comme en mode centralisé). Cela étend considérablement la prise en charge des VPN au-delà des capacités VPN centralisées et offre une haute disponibilité. Le VPN S2S distribué s'exécute sur une grappe allant jusqu'à deux châssis, chacun contenant jusqu'à trois modules (six membres de grappe au total), chaque module prenant en charge jusqu'à 6 000 sessions actives (12 000 au total), pour un maximum d'environ 36 000 sessions actives (72 000 au total). Écrans nouveaux ou modifiés : **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > ASA Cluster (Grappe ASA) > VPN Cluster Summary (Résumé de la grappe VPN)** **Monitoring (Supervision) > VPN > VPN Statistics (Statistiques de VPN) > Sessions** **Configuration > Device Management (Gestion des périphériques) > High Availablility and Scalability (Haute disponibilité et évolutivité) > ASA Cluster (Grappe ASA)** **Wizards (Assistants) > Site-to-Site (Site à site)** **Monitoring (Supervision) > VPN > VPN Statistics (Statistiques de VPN) > Sessions** **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > ASA Cluster (Grappe ASA) > VPN Cluster Summary (Résumé de la grappe VPN)** **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > ASA Cluster (Grappe ASA) > System Resource Graphs (Graphique de ressources du système) > CPU/Memory (Processeur/mémoire)** **Monitoring (Supervision) > Logging (Journalisation) > Real-Time Log Viewer (Visionneuse de journal en temps réel)**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Détection améliorée des échecs de vérification de l'intégrité de l'unité de grappe	9.8(1)	Vous pouvez maintenant configurer un délai de rétention inférieur pour la vérification de l'intégrité de l'unité : 0,3 seconde au minimum. La valeur minimum précédente était de 0,8 seconde. Cette fonctionnalité modifie le schéma de messagerie de vérification de l'intégrité de l'unité pour passer des *keepalives* dans le plan de commande aux *heartbeats* dans le plan de données. L'utilisation de pulsations améliore la fiabilité et la réactivité de la mise en grappe en évitant les problèmes liés à la surcharge du processeur du plan de commande et aux retards de planification. Notez que la configuration d'un délai de rétention inférieur augmente l'activité de messagerie de la liaison de commande de grappe. Nous vous suggérons d'analyser votre réseau avant de configurer un faible délai de rétention. Par exemple, assurez-vous que l'envoi d'un message Ping d'une unité à une autre via la liaison de commande de grappe retourne dans le *holdtime*/3, car il y aura trois messages de pulsation au cours d'un intervalle de délai de rétention. Si vous rétrogradez votre logiciel ASA après avoir défini le délai de rétention sur 0,3–0,7, ce paramètre reviendra à la valeur par défaut de 3 secondes, car le nouveau paramètre n'est pas pris en charge. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**
Délai anti-rebond configurable pour marquer une interface comme défaillante pour le Châssis Firepower 4100/9300	9.8(1)	Vous pouvez maintenant configurer le délai antirebond avant que l'ASA considère une interface comme défaillante et que l'unité ne soit supprimée de la grappe. Cette fonctionnalité permet une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié avant de marquer l'interface comme défaillante, et l'unité est supprimée de la grappe. Le délai antirebond par défaut est de 500 ms, avec une plage de 300 ms à 9 secondes. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**
Amélioration de la mise en grappe inter-sites pour l'ASA sur le Châssis Firepower 4100/9300	9.7(1)	Vous pouvez maintenant configurer l'ID de site pour chaque Châssis Firepower 4100/9300 lorsque vous déployez la grappe ASA. Auparavant, vous deviez configurer l'ID de site dans l'application ASA; cette nouvelle fonctionnalité facilite le déploiement initial. Notez que vous ne pouvez plus définir l'ID de site dans la configuration ASA. En outre, pour une meilleure compatibilité avec la mise en grappe inter-sites, nous vous recommandons de mettre à niveau vers ASA 9.7(1) et FXOS 2.1.1, ce qui comprend plusieurs améliorations de la stabilité et des performances. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Localisation de directeur : amélioration de la mise en grappe inter-sites pour les centres de données	9.7(1)	Pour améliorer les performances et conserver le trafic sur un site de mise en grappe inter-sites pour les centres de données, vous pouvez activer la localisation de directeur. Les nouvelles connexions sont généralement équilibrées et appartiennent aux membres de la grappe d'un site donné. Cependant, l'ASA attribue le rôle de directeur à un membre sur *n'importe quel* site. La localisation du directeur permet des rôles de directeur supplémentaires : un directeur local sur le même site que le propriétaire et un directeur global qui peut se trouver sur n'importe quel site. Le fait de maintenir le propriétaire et le directeur sur le même site améliore les performances. En cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site. Le directeur global est utilisé si un membre d'une grappe reçoit des paquets pour une connexion appartenant à un autre site. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **Cluster Configuration (Configuration de la grappe)**
Prise en charge de 16 châssis pour le Firepower 4100	9.6(2)	Vous pouvez maintenant ajouter jusqu'à 16 châssis à la grappe pour le Firepower 4100. Nous n'avons pas modifié d'écrans.
Prise en charge de Firepower 4100	9.6(1)	Avec FXOS 1.1.4, l'ASA prend en charge la mise en grappe inter-châssis sur le Firepower 4100 pour un maximum de 6 châssis. Nous n'avons pas modifié d'écrans.
Prise en charge des adresses IP spécifiques au site en mode routé avec EtherChannel étendu	9.6(1)	Pour la mise en grappe inter-sites en mode routé avec les canaux EtherChannels étendus, vous pouvez désormais configurer l'adresse IP spécifique au site en plus des adresses MAC spécifiques au site. L'ajout d'adresses IP de site vous permet d'utiliser l'inspection ARP sur les périphériques Overlay Transport Virtualization (OTV) pour empêcher les réponses ARP de l'adresse MAC globale de circuler sur l'interconnexion de centre de données (DCI), ce qui peut causer des problèmes de routage. L'inspection ARP est requise pour certains commutateurs qui ne peuvent pas utiliser de VACL pour filtrer les adresses MAC. Nous avons modifié l'écran suivant : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add/Edit EtherChannel Interface (Ajouter/Modifier l'interface EtherChannel)** > **Advanced (Avancé)**
Mise en grappe inter-châssis pour 16 modules et mise en grappe inter-sites pour l'application ASA Firepower 9300	9.5(2.1)	Grâce à FXOS 1.1.3, vous pouvez désormais activer la mise en grappe inter-châssis et par extension inter-sites. Vous pouvez inclure jusqu'à 16 modules. Par exemple, vous pouvez utiliser 1 module dans 16 châssis, ou 2 modules dans 8 châssis, ou toute combinaison qui fournit un maximum de 16 modules. Nous n'avons pas modifié d'écrans.
Adresses MAC spécifiques au site pour la prise en charge de la mise en grappe inter-sites pour EtherChannel étendu en mode de pare-feu routé	9.5(2)	Vous pouvez désormais utiliser la mise en grappe inter-sites pour les EtherChannels étendus en mode routé. Pour éviter le basculement des adresses MAC, configurez un ID de site pour chaque membre d'une grappe afin qu'une adresse MAC propre au site pour chaque interface puisse être partagée entre les unités d'un site. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Personnalisation de la grappe ASA du comportement de reconnexion automatique en cas de défaillance d'une interface ou de la liaison de commande de grappe	9.5(2)	Vous pouvez désormais personnaliser le comportement de reconnexion automatique en cas de défaillance d'une interface ou de la liaison de commande de grappe. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Auto Rejoin (Reconnexion automatique)**
La grappe ASA prend en charge GTPv1 et GTPv2	9.5(2)	La grappe ASA prend désormais en charge l'inspection GTPv1 et GTPv2. Nous n'avons pas modifié d'écrans.
Délai de réplication de la grappe pour les connexions TCP	9.5(2)	Cette fonctionnalité aide à éliminer le « travail inutile » lié aux flux de courte durée en retardant la création du flux directeur/de sauvegarde. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster Replication (Réplication de grappe ASA)**
Inspection LISP pour la mobilité des flux inter-sites	9.5(2)	L'architecture Cisco Locator/Protocole de séparation d'ID (LISP) sépare l'identité de l'appareil de son emplacement dans deux espaces de numérotation différents, ce qui rend la migration du serveur transparente pour les clients. L'ASA peut inspecter le trafic LISP pour détecter les changements d'emplacement, puis utiliser ces renseignements pour un fonctionnement de mise en grappe transparent; les membres de la grappe ASA inspectent le trafic LISP passant entre le routeur de premier saut et le routeur de tunnel de sortie (ETR) ou le routeur de tunnel de sortie (ITR), puis changent le propriétaire du flux pour qu'il se trouve sur le nouveau site. Nous avons introduit ou modifié les écrans suivants : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)** **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **LISP** **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)** > **Protocol Inspection (Inspection de protocole)** **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)** > **Cluster (Grappe)** **Monitoring (Supervision)** > **Routing (Routage)** > **LISP-EID Table (Tableau LISP-EID)**
Les améliorations de la NAT de classe opérateur sont désormais prises en charge dans le basculement et la mise en grappe d'ASA	9.5(2)	Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois (Voir RFC 6888). Cette fonctionnalité est désormais prise en charge dans les déploiements de basculement et de grappe ASA. Nous n'avons pas modifié d'écrans.

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Niveau configurable pour la mise en grappe des entrées de trace	9.5(2)	Par défaut, tous les niveaux d'événements de mise en grappe sont inclus dans le tampon de trace, y compris de nombreux événements de bas niveau. Pour limiter la trace aux événements de niveau supérieur, vous pouvez définir le niveau de trace minimum pour la grappe. Nous n'avons pas modifié d'écrans.
Mise en grappe d'ASA intra-châssis pour le Firepower 9300	9.4(1.150)	Vous pouvez mettre en grappe jusqu'à 3 modules de sécurité dans le châssis Firepower 9300. Tous les modules dans le châssis doivent appartenir à la grappe. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster Replication (Réplication de grappe ASA)**



CHAPITRE 14

Grappe ASA pour l'ASA virtuel pour le cloud privé

La mise en grappe vous permet de regrouper plusieurs ASA virtuel en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques. Vous pouvez déployer les grappes ASA virtuel à l'aide de :

- KVM
- VMware

Remarque Seul le mode pare-feu routé est pris en charge.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités non prises en charge par la mise en grappe, à la page 590.

- À propos de la mise en grappe d'ASA virtuel, à la page 548
- Licences pour la mise en grappe d'ASA virtuel, à la page 555
- Exigences et conditions préalables à la mise en grappe d'ASA virtuel, à la page 555
- Lignes directrices de la mise en grappe d'ASA virtuel, à la page 556
- Configurer la mise en grappe d'ASA virtuel à l'aide d'une configuration Day0, à la page 557
- Configurer la mise en grappe ASA virtuel après le déploiement, à la page 560
- Personnaliser l'opération de mise en grappe, à la page 571
- Gérer les nœuds de la grappe, à la page 580
- Supervision de la grappe ASA virtuel, à la page 586
- Exemples de mise en grappe d'ASA virtuel, à la page 588
- Référence pour la mise en grappe, à la page 589
- Historique de la mise en grappe d'ASA virtuel, à la page 607

À propos de la mise en grappe d'ASA virtuel

Cette section décrit l'architecture de mise en grappe et son fonctionnement.

Intégration de la grappe dans votre réseau

La grappe se compose de plusieurs pare-feu agissant comme un seul périphérique. Pour agir comme une grappe, les pare-feu ont besoin de l'infrastructure suivante :

- Réseau isolé pour la communication intra-grappe, appelé *liaison de commande de grappe*, qui utilise des interfaces VXLAN. Les VXLAN, qui agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3, permettent à la ASA Virtual d'envoyer des messages en diffusion ou en multidiffusion sur la liaison de commande de grappe.
- Accès de gestion à chaque pare-feu pour la configuration et la surveillance. Le déploiement ASA Virtual comprend une interface de gestion Management 0/0 que vous utiliserez pour gérer les nœuds de la grappe.

Lorsque vous placez la grappe dans votre réseau, les routeurs en amont et en aval doivent être en mesure d'équilibrer la charge des données entrant et provenant de la grappe à l'aide des interfaces individuelles de couche 3 et de l'une des méthodes suivantes :

- Routage basé sur les politiques : les routeurs en amont et en aval équilibrent la charge entre les nœuds à l'aide de cartes de routage et de listes de contrôle d'accès.
- Routage à chemins multiples à coût égal : les routeurs en amont et en aval effectuent l'équilibrage de la charge entre les nœuds à l'aide de routes statiques ou dynamiques à coût égal.

Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge.

Nœuds de la grappe

Les membres du nœud collaborent pour partager la politique de sécurité et les flux de trafic. Cette section décrit la nature du rôle de chaque nœud.

Configuration du démarrage

Sur chaque appareil, vous configurez une configuration de démarrage minimale qui inclut le nom de la grappe, l'interface de la liaison de commande de grappe et les autres paramètres de la grappe. Le premier nœud sur lequel vous activez la mise en grappe devient généralement le nœud de *contrôle*. Lorsque vous activez la mise en grappe sur les nœuds suivants, ils rejoignent la grappe en tant que nœuds de *données*.

Rôles des nœuds de contrôle et de données

Un membre de la grappe est le nœud de contrôle. Si plusieurs nœuds de la grappe sont mis en ligne en même temps, le nœud de contrôle est déterminé par le paramètre de priorité dans la configuration de démarrage. La priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée. Tous les autres membres sont des nœuds

de données. En règle générale, lorsque vous créez une grappe pour la première fois, le premier nœud que vous ajoutez devient le nœud de contrôle simplement parce que c'est le seul nœud de la grappe à ce moment-là.

Vous devez effectuer toute la configuration (à l'exception de la configuration de démarrage) sur le nœud de contrôle uniquement; la configuration est ensuite reproduite sur les nœuds de données. Dans le cas de ressources physiques, telles que les interfaces, la configuration du nœud de contrôle est reflétée sur tous les nœuds de données. Par exemple, si vous configurez Ethernet 1/2 comme interface interne et Ethernet 1/1 comme interface externe, ces interfaces sont également utilisées sur les nœuds de données en tant qu'interfaces interne et externe.

Certaines fonctionnalités ne sont pas évolutives en grappe, et le nœud de contrôle gère tout le trafic pour ces fonctionnalités.

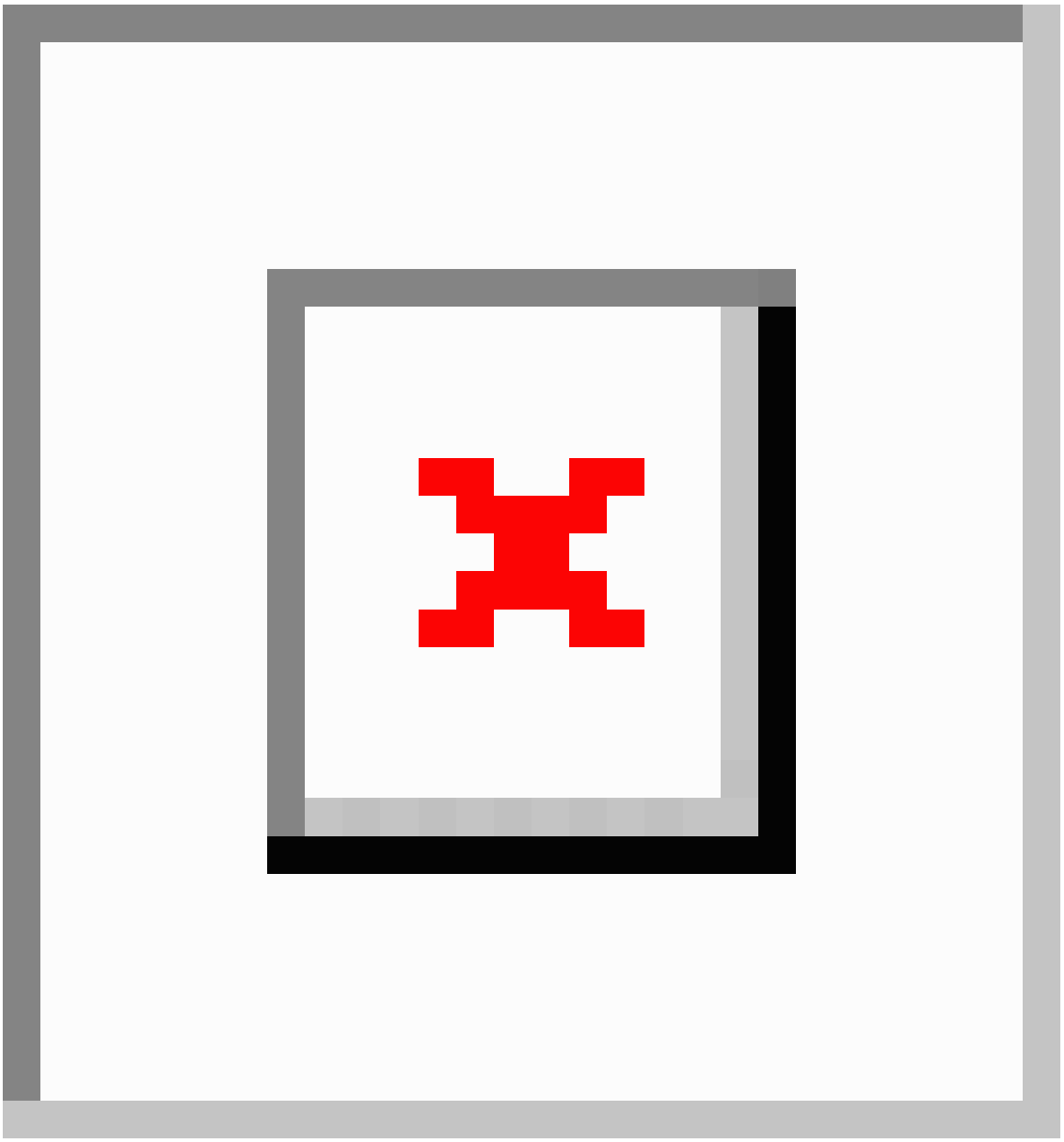
Interfaces individuelles

Vous pouvez configurer les interfaces de grappe en tant *qu'interfaces individuelles*.

Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre *adresse IP locale* utilisée pour le routage. L'*adresse IP de la grappe principale* pour chaque interface est une adresse fixe qui appartient toujours au nœud de contrôle. Lorsque le nœud de contrôle change, l'adresse IP de la grappe principale est déplacée vers le nouveau nœud de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente.

Comme la configuration de l'interface doit être configurée uniquement sur le nœud de contrôle, vous configurez un ensemble d'adresses IP à utiliser pour une interface donnée sur les nœuds de la grappe, y compris un pour le nœud de contrôle.

L'équilibrage de charge doit être configuré séparément sur le commutateur en amont.



Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge.

Routage à base de règles

Lorsque vous utilisez des interfaces individuelles, chaque interface ASA conserve ses propres adresses IP et MAC. Une méthode d'équilibrage de la charge est le routage basé sur les politiques (PBR).

Nous vous recommandons cette méthode si vous utilisez déjà PBR et que vous souhaitez tirer parti de votre infrastructure existante.

PBR prend des décisions de routage en fonction d'une carte de routage et d'une ACL. Vous devez répartir manuellement le trafic entre toutes les ASA d'une grappe. Comme PBR est statique, il se peut qu'il ne permette pas d'atteindre un résultat d'équilibrage de la charge optimale à tout moment. Pour obtenir les meilleures performances, nous vous recommandons de configurer la politique PBR de sorte que les paquets d'acheminement et de retour d'une connexion soient dirigés vers la même ASA.

Par exemple, si vous avez un routeur Cisco, la redondance peut être obtenue en utilisant Cisco IOS PBR avec Object Tracking. Le suivi d'objets Cisco IOS surveille chaque ASA à l'aide d'un ping ICMP. PBR peut ensuite activer ou désactiver les cartes de routage en fonction de l'accessibilité d'un ASA.

Routage à chemins multiples à coût égal

Lorsque vous utilisez des interfaces individuelles, chaque interface ASA conserve ses propres adresses IP et MAC. Le routage à chemins multiples à coûts égaux (ECMP) est une méthode d'équilibrage de la charge.

Nous vous recommandons cette méthode si vous utilisez déjà ECMP et que vous souhaitez tirer parti de votre infrastructure existante.

Considérations sur le routage ECMP

Le routage ECMP peut transférer des paquets sur plusieurs « meilleurs chemins » qui se partagent la première place dans la mesure du routage. Comme pour l'EtherChannel, un hachage des adresses IP source et de destination ou des ports source et de destination peut être utilisé pour envoyer un paquet vers l'un des sauts suivants.

Si vous utilisez des routes statiques pour le routage ECMP, la défaillance de l'ASA peut provoquer des problèmes. le routage continue d'être utilisé et le trafic vers l'ASA défaillant sera perdu.

Si vous utilisez des routes statiques, veillez à utiliser une fonctionnalité de surveillance de routage statique telle que le suivi d'objets. Nous recommandons d'utiliser des protocoles de routage dynamique pour ajouter et supprimer des routes, auquel cas vous devez configurer chaque ASA pour qu'il participe au routage dynamique.

Liaison de commande de grappe

Chaque nœud doit dédier une interface en tant qu'interface VXLAN (VTEP) pour la liaison de commande de grappe. Pour en savoir plus sur VXLAN, consultez Interfaces VXLAN, à la page 669.

Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP comporte deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier), et une interface normale appelée interface source du VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

Interface de la source VTEP

L'interface source du VTEP est une interface ASA Virtual classique à laquelle vous prévoyez associer l'interface VNI. Vous pouvez configurer une interface source de VTEP pour qu'elle agisse en tant que liaison de commande de grappe. L'interface source est réservée à une utilisation avec la liaison de commande de grappe uniquement. Chaque interface source de VTEP possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

Interface VNI

Une interface VNI est semblable à une interface VLAN : il s'agit d'une interface virtuelle qui sépare le trafic réseau sur une interface physique donnée au moyen de balisage. Vous ne pouvez configurer qu'une seule interface VNI. Chaque interface VNI possède une adresse IP sur le même sous-réseau.

VTEP homologues

Contrairement au VXLAN habituel pour les interfaces de données, qui autorise un seul homologue VTEP, la mise en grappe ASA Virtual vous permet de configurer plusieurs homologues.

Présentation du trafic de liaison de commande de grappe

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

Échec de la liaison de commande de grappe

Si le protocole de liaison de commande de grappe tombe en panne pour une unité, la mise en grappe est désactivée; les interfaces de données sont fermées. Après avoir corrigé la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.

Remarque Lorsque l'ASA virtuel devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que l'unité a reçue du DHCP ou de l'ensemble d'adresses IP de la grappe. Si vous utilisez un ensemble d'adresses IP de grappe, si vous rechargez et que l'unité est toujours inactive dans la grappe, l'interface de gestion n'est pas accessible (car elle utilise alors l'adresse IP principale, qui est la même que le nœud de contrôle). Vous devez utiliser le port de console (si disponible) pour toute autre configuration.

Test de ping de la MTU de la liaison de commande de grappe

Utilisez les tests ping MTU de liaison de commande de grappe pour

- vérifier la compatibilité de l'unité de transfert vérifier la compatibilité de la MTU entre les nœuds de la grappe au cours du processus de jonction,
- utiliser des tests de fragmentation basés sur le ping pour confirmer que le chemin réseau prend en charge le traitement approprié des paquets, et

- permettre aux nœuds de rejoindre la grappe même si les tests échouent, tout en fournissant des messages de diagnostic pour le dépannage des incompatibilités de MTU.

Lorsqu'un nœud rejoint la grappe, le nœud de contrôle envoie un ping avec une charge utile d'une taille égale à deux fois la MTU. Ce processus teste la capacité du réseau à gérer la fragmentation des paquets, car la couche IP sous-jacente fragmentera les paquets qui dépassent la limite de MTU.

Un ping réussi confirme que le chemin réseau prend en charge une fragmentation appropriée et que la liaison de commande de grappe peut traiter de manière fiable le trafic avec la MTU configurée.

Si le ping échoue, affichez ces messages :

- **show cluster history**—`Événement : échec du test CCL MTU pour l'unité name`
- Console AVERTISSEMENT—`AVERTISSEMENT : L'unité name n'est pas accessible dans le test ICMP de trame étendue CCL, veuillez vérifier l'interface de grappe et la configuration MTU du commutateur.`

Même si le message ping échoue, le nœud est autorisé à rejoindre la grappe. Dans ce cas, vous devez résoudre la non-concordance de MTU dès que possible.

Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

Gestion des grappes ASA virtuel

L'un des avantages de l'utilisation de la mise en grappe ASA virtuel est la facilité de gestion. Cette section décrit comment gérer la grappe.

Réseau de gestion

Nous vous conseillons de connecter tous les nœuds à un seul réseau de gestion. Ce réseau est distinct de la liaison de commande de grappe.

Interface de gestion

Utilisez l'interface Management 0/0 pour la gestion.

Remarque Vous ne pouvez pas activer le routage dynamique pour l'interface de gestion. Vous devez utiliser une route statique.

Vous pouvez utiliser l'adressage statique ou DHCP pour l'adresse IP de gestion.

Si vous utilisez l'adressage statique, vous pouvez utiliser l'adresse IP de la grappe principale qui est une adresse fixe pour la grappe qui appartient toujours au nœud de contrôle actuel. Pour chaque interface, vous configurez également une plage d'adresses de sorte que chaque nœud, y compris le nœud de contrôle actuel, puisse utiliser une adresse locale de la plage. L'adresse IP de la grappe principale fournit un accès de gestion

cohérent à une adresse; lorsqu'un nœud de contrôle change, l'adresse IP de la grappe principale est déplacée vers le nouveau nœud de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente. L'adresse IP locale est utilisée pour le routage et est également utile pour la résolution de problèmes. Par exemple, vous pouvez gérer la grappe en vous connectant à l'adresse IP de la grappe principale, qui est toujours associée au nœud de contrôle actuel. Pour gérer un membre, vous pouvez vous connecter à l'adresse IP locale. Pour le trafic de gestion sortant tel que TFTP ou le journal système, chaque nœud, y compris le nœud de contrôle, utilise l'adresse IP locale pour se connecter au serveur.

Si vous utilisez DHCP, vous n'utilisez pas un ensemble d'adresses locales ou n'avez pas d'adresse IP de grappe principale.

Remarque Le trafic vers la boîte doit être acheminé vers l'adresse IP de gestion du nœud; le trafic vers la boîte n'est pas transféré sur la liaison de commande de grappe vers un autre nœud.

Gestion de nœud de contrôle vs Gestion de nœud de données

La gestion et la surveillance peuvent avoir lieu sur le nœud de contrôle. À partir du nœud de contrôle, vous pouvez vérifier les statistiques d'exécution, l'utilisation des ressources ou d'autres informations de surveillance sur tous les nœuds. Vous pouvez également transmettre une commande à tous les nœuds de la grappe et reproduire les messages de console des nœuds de données vers le nœud de contrôle.

Vous pouvez surveiller directement les nœuds de données si vous le souhaitez. Bien que cela soit également disponible à partir du nœud de contrôle, vous pouvez effectuer la gestion de fichiers sur les nœuds de données (y compris la sauvegarde de la configuration et la mise à jour des images). Les fonctions suivantes ne sont pas disponibles à partir du nœud de commande :

- Surveillance des statistiques propres à la grappe par nœud.
- Surveillance des journaux système par nœud (sauf pour les journaux système envoyés à la console lorsque la duplication de la console est activée).
- SNMP
- NetFlow

duplication de clé de chiffrement

Lorsque vous créez une clé de chiffrement sur le nœud de contrôle, la clé est répliquée sur tous les nœuds de données. Si vous avez une session SSH sur l'adresse IP de la grappe principale, vous serez déconnecté en cas de défaillance du nœud de contrôle. Le nouveau nœud de contrôle utilise la même clé pour les connexions SSH, de sorte que vous n'avez pas besoin de mettre à jour la clé d'hôte SSH mise en cache lorsque vous vous reconnectez au nouveau nœud de contrôle.

Incompatibilité d'adresse IP du certificat de connexion ASDM

Par défaut, un certificat autosigné est utilisé pour la connexion ASDM en fonction de l'adresse IP locale. Si vous vous connectez à l'adresse IP de la grappe principale à l'aide d'ASDM, un message d'avertissement concernant une adresse IP non concordante peut s'afficher, car le certificat utilise l'adresse IP locale, et non l'adresse IP de la grappe principale. Vous pouvez ignorer le message et établir la connexion ASDM. Cependant, pour éviter ce type d'avertissement, vous pouvez inscrire un certificat qui contient l'adresse IP de la grappe principale et toutes les adresses IP locales de l'ensemble d'adresses IP. Vous pouvez ensuite utiliser ce certificat

pour chaque membre de la grappe. Consultez https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html pour de plus amples renseignements.

Mise en grappe inter-sites

Pour les installations inter-sites, vous pouvez profiter de la mise en grappe d'ASA virtuel tant que vous suivez les lignes directrices recommandées.

Vous pouvez configurer chaque châssis de grappe pour qu'il appartienne à un ID de site distinct. Les ID de site sont utilisés pour permettre la mobilité de flux à l'aide de l'inspection LISP, la localisation du directeur pour améliorer les performances et réduire la latence aller-retour pour la mise en grappe inter-sites pour les centres de données, et la redondance des sites pour les connexions où un propriétaire de secours d'un flux se trouve toujours sur un autre site que celui du propriétaire.

Consultez les sections suivantes pour en savoir plus sur la mise en grappe inter-sites :

- Dimensionnement de l'interconnexion du centre de données : Exigences et conditions préalables à la mise en grappe d'ASA virtuel, à la page 555
- Lignes directrices inter-sites : Lignes directrices de la mise en grappe d'ASA virtuel, à la page 556
- Configurer la mobilité des flux de grappes : Configurer la mobilité des flux de grappes, à la page 577
- Activer la localisation du directeur : Configurer les paramètres de grappe ASA de base, à la page 571
- Activer la redondance de site : Configurer les paramètres de grappe ASA de base, à la page 571
- Exemples inter-sites : Exemple inter-sites nord-sud de mode routé d'interface individuelle, à la page 588

Licences pour la mise en grappe d'ASA virtuel

Chaque nœud de grappe nécessite la même licence de modèle. Nous vous conseillons d'utiliser le même nombre de CPU et de mémoire pour tous les nœuds, sinon les performances seront limitées sur tous les nœuds pour correspondre au membre le moins performant. Le niveau de débit sera répliqué du nœud de contrôle à chaque nœud de données afin qu'ils correspondent.

Remarque Si vous annulez l'enregistrement de l'ASA virtuel pour qu'il ne soit pas sous licence, il reviendra à un état de débit fortement limité si vous rechargez l'ASA virtuel. Un nœud de grappe sans licence et à faible performance aura une incidence négative sur les performances de l'ensemble de la grappe. Assurez-vous de conserver tous les nœuds de la grappe sous licence ou de supprimer les nœuds sans licence.

Exigences et conditions préalables à la mise en grappe d'ASA virtuel

Exigences du modèle

- ASAv30, ASAv50, ASAv100

- Les services en cloud privé suivants :
  - KVM
  - VMware
- Un maximum de 16 nœuds dans une grappe sur *deux* hôtes dans une configuration de déploiement 2 x 8. Nous vous conseillons de déployer un maximum de *huit* ASAv sur chacun des *deux* hôtes (2 x 8), ce qui donne une grappe de 16 nœuds.

Plateforme ASA virtuel et configuration logicielle requise

Tous les nœuds d'une grappe :

- Il doit s'agir du même modèle. Nous vous conseillons d'utiliser le même nombre de CPU et de mémoire pour tous les nœuds, sinon les performances seront limitées sur tous les nœuds pour correspondre au nœud le moins performant.
- Doit exécuter le logiciel identique, sauf lors d'une mise à niveau d'image. La mise à niveau rapide est prise en charge. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.
- Les nouveaux membres de la grappe doivent utiliser le même paramètre de chiffrement SSL (la commande **ssl encryption**) que le nœud de contrôle pour la communication de la liaison de commande de grappe initiale avant la réplication de la configuration.

Lignes directrices de la mise en grappe d'ASA virtuel

Basculement

Le basculement n'est pas pris en charge avec la mise en grappe.

IPv6

La liaison de commande de grappe est uniquement prise en charge avec IPv4.

Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, activation ou désactivation d'une interface sur l'ASA ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité de l'interface.
- Lors de l'ajout d'un nœud à une grappe existante ou lors du rechargement d'un nœud, il se produit une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent bloquer votre connexion; par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.

- Nous ne prenons pas en charge les VXLAN pour les interfaces de données; seule la liaison de commande de grappe prend en charge VXLAN.
- Il faut du temps pour répliquer les modifications sur toutes les unités d'une grappe. Si vous apportez une modification importante, par exemple, ajouter une règle de contrôle d'accès qui utilise des groupes d'objets (qui, lorsqu'ils sont déployés, sont divisés en plusieurs règles), le temps nécessaire pour effectuer la modification peut dépasser le délai d'expiration des nœuds de la grappe avec un message de réussite. Si cela se produit, vous pourriez voir le message « Échec de la réplication de la commande ». Vous pouvez ignorer le message.

Valeurs par défaut pour la mise en grappe d'ASA virtuel

- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- La fonction de jonction automatique de la grappe en cas d'échec de la liaison de commande de grappe offre des tentatives illimitées toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante effectue 3 essais toutes les 5 minutes, l'intervalle croissant étant fixé à 2.
- Le rééquilibrage de la connexion est désactivé par défaut. Si vous activez le rééquilibrage de la connexion, l'intervalle par défaut entre les échanges d'informations de chargement est de 5 secondes.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe d'ASA virtuel à l'aide d'une configuration Day0

Configuration Day0 du nœud de contrôle

La configuration Day0 suivante pour le nœud de contrôle comprend la configuration de démarrage suivie de la configuration d'interface qui sera répliquée sur les nœuds de données. Le texte en gras affiche les valeurs que vous devez modifier pour la configuration Day0 du nœud de données.



Remarque Cette configuration comprend uniquement la configuration centré sur la grappe. Votre configuration Day0 doit également inclure d'autres paramètres pour les licences, l'accès SSH , l'accès ASDM , etc. Consultez le guide de démarrage pour en savoir plus sur les configurations Day0.

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
network-object host 10.6.6.53
network-object host 10.6.6.54
```

```
!
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
security-level 0
ip address 10.6.6.51 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
peer-group cluster-peers
!
! Management Interface Using DHCP
interface management 0/0
nameif management
ip address dhcp setroute
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
local-unit A
cluster-interface vni1 ip 10.2.2.1 255.255.255.0
priority 1
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
```

```
!
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

Configuration Day0 du nœud de données

La configuration Day0 suivante pour le nœud de données inclut uniquement la configuration de démarrage. Le texte en gras affiche les valeurs que vous devez modifier à partir de la configuration Day0 du nœud de contrôle.

Remarque Cette configuration comprend uniquement la configuration centré sur la grappe. Votre configuration Day0 doit également inclure d'autres paramètres pour les licences, l'accès SSH , l'accès ASDM , etc. Consultez le guide de démarrage pour en savoir plus sur les configurations Day0.

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
network-object host 10.6.6.53
network-object host 10.6.6.54
!
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
security-level 0
ip address 10.6.6.52 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
peer-group cluster-peers
!
! Management Interface Using DHCP
interface management 0/0
nameif management
ip address dhcp setroute
```

```
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
local-unit B
cluster-interface vni1 ip 10.2.2.2 255.255.255.0
priority 2
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
!
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

Configurer la mise en grappe ASA virtuel après le déploiement

Pour configurer la mise en grappe après avoir déployé vos ASA virtuel, effectuez les tâches suivantes.

Sauvegarder vos configurations (conseillé)

Lorsque vous activez la mise en grappe sur une unité de données, la configuration actuelle est remplacée par une configuration synchronisée à partir de l'unité active. Si vous souhaitez quitter complètement la grappe, il peut être utile d'avoir une configuration de sauvegarde avec une configuration d'interface de gestion utilisable.

Avant de commencer

Effectuez une sauvegarde sur chaque unité.

Procédure

Étape 1 Choisissez **Tools (Outils)** > **Backup Configurations (Configurations de sauvegarde)**.

Étape 2 Sauvegardez au moins la configuration en cours d'exécution. Consultez Sauvegarde et restauration de configurations ou d'autres fichiers, à la page 1203 pour connaître la procédure détaillée.

Configurer les paramètres d'interface

Configurez le mode d'interface de grappe ainsi que les interfaces sur le nœud de contrôle. La configuration d'interface sera répliquée sur les nœuds de données lorsqu'ils rejoignent la grappe. Notez que la configuration de la laision de commande de grappe est traitée dans la procédure de configuration de démarrage.

Configurer le mode d'interface de grappe sur le nœud de contrôle

Avant d'activer la mise en grappe, vous devez convertir le pare-feu pour utiliser des interfaces individuelles. Étant donné que la mise en grappe limite les types d'interfaces que vous pouvez utiliser, ce processus vous permet de vérifier votre configuration existante pour détecter les interfaces incompatibles, puis vous empêche de configurer des interfaces non prises en charge.

Remarque Si vous n'ajoutez pas de nœuds de données à partir du nœud de contrôle, vous devez définir le mode d'interface manuellement sur tous les nœuds en fonction de cette section, pas seulement sur le nœud de contrôle; si vous ajoutez des nœuds de données à partir du nœud de contrôle, ASDM définit automatiquement le mode d'interface sur le nœud de données.

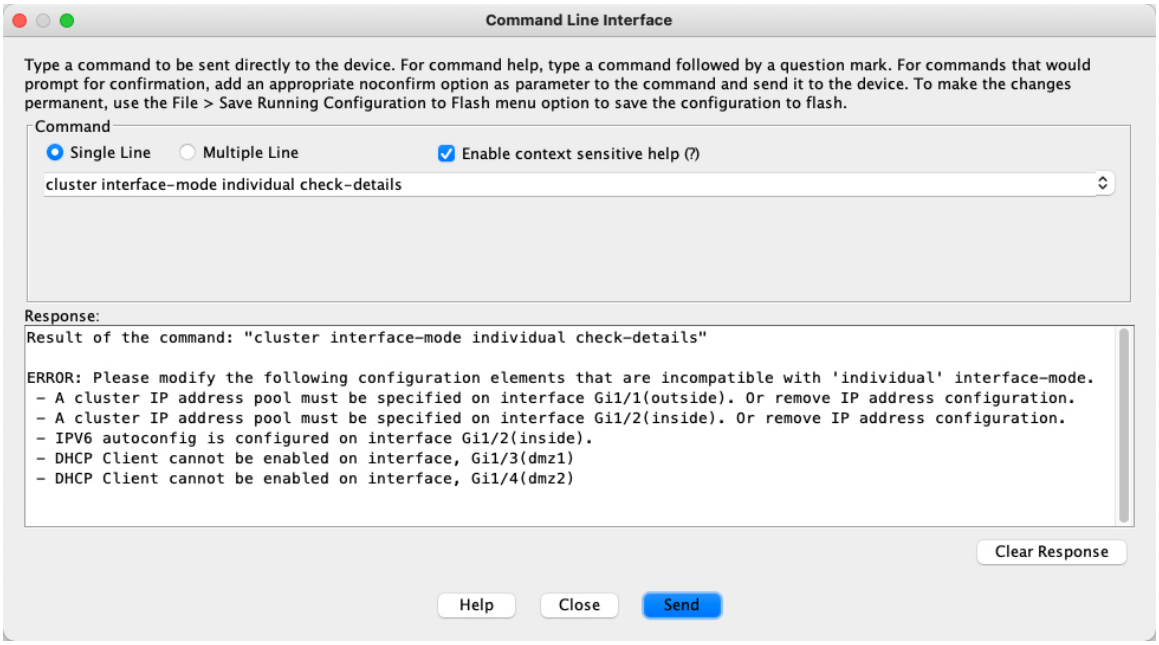
Procédure

Étape 1 Dans ASDM sur le nœud de contrôle, choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.Affichez toute configuration incompatible afin de pouvoir forcer le mode d'interface et corriger votre configuration ultérieurement; le mode n'est pas modifié avec cette commande :

cluster interface-mode individual check-details

Exemple :

Illustration 64 : Sortie de l'interface de commande en ligne



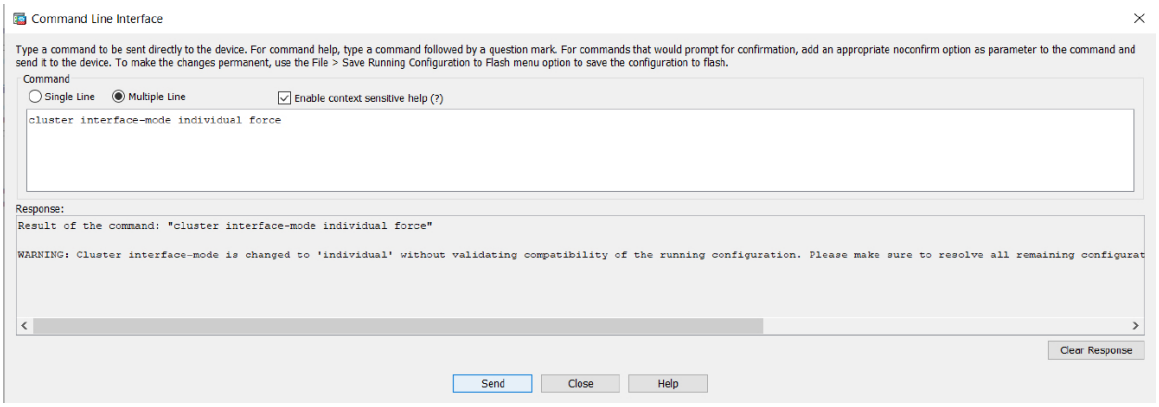
Mise en garde Après avoir défini le mode d'interface, vous pouvez continuer à vous connecter à l'interface; cependant, si vous rechargez l'ASA avant de configurer votre interface de gestion pour respecter les exigences de mise en grappe (par exemple, ajout d'un ensemble d'adresses IP de grappe ou obtention de l'adresse IP de DHCP), vous ne pourrez pas vous reconnecter, car la configuration d'interface incompatible avec la grappe est supprimée. Dans ce cas, vous devrez vous connecter au port de console, si disponible, pour corriger la configuration d'interface.

Étape 2 Définissez le mode d'interface pour la mise en grappe :

cluster interface-mode individual force

Exemple :

Illustration 65 : Définir le mode d'interface



Il n'y a pas de paramètres par défaut; vous devez choisir explicitement le mode. Si vous n'avez pas défini le mode, vous ne pouvez pas activer la mise en grappe.

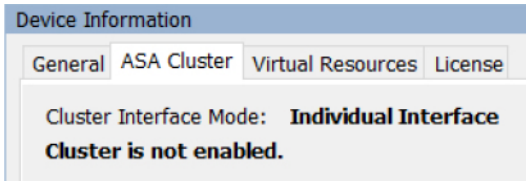
L'option **force** change le mode sans vérifier si votre configuration comporte des paramètres incompatibles. Vous devez résoudre manuellement tous les problèmes de configuration après avoir changé de mode. Étant donné que toute configuration d'interface ne peut être corrigée qu'après avoir défini le mode, nous vous conseillons d'utiliser l'option **force** afin de pouvoir au moins partir de la configuration existante. Vous pouvez réexécuter l'option **check-details** après avoir défini le mode pour obtenir plus de conseils.

Sans l'option **force**, en cas de configuration incompatible, vous êtes invité à effacer votre configuration et à la recharger, ce qui vous obligera à vous connecter au port de console (si disponible) pour reconfigurer votre accès de gestion. Si votre configuration est compatible (ce qui est rare), le mode est modifié et la configuration est conservée. Si vous ne souhaitez pas effacer votre configuration, vous pouvez quitter la commande en tapant **n**.

Pour supprimer le mode d'interface, saisissez la commande **no cluster interface-mode**.

Étape 3 Quittez ASDM et rechargez. ASDM doit être redémarré pour prendre correctement en compte le mode d'interface de la grappe. Après le rechargement, vous verrez l'onglet ASA Cluster (Grappe ASA) sur la page d'accueil :

Illustration 66 : ASDM doit être mis à jour



Configurer la liaison de commande de grappe sur le nœud de contrôle

Configurez une interface VXLAN pour l'interface de liaison de commande de grappe avant d'exécuter l'assistant. Pour en savoir plus sur VXLAN et la liaison de commande de grappe, consultez Liaison de commande de grappe, à la page 551.

Avant de commencer

Activez la réservation de bâti grand format pour une utilisation avec la liaison de commande de grappe, afin de pouvoir définir la MTU de la liaison de commande de grappe à la valeur conseillée. L'activation des bâtis grand format entraîne le rechargement de l'ASA. Consultez l'écran **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.

Remarque Vous devez activer la réservation de bâti grand format sur chaque nœud séparément.

Procédure

Étape 1 Identifiez les adresses IP des homologues du terminal de tunnel VXLAN (VTEP) dans un groupe d'objets réseau.

Consultez la page **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Objects/Groups (Objets réseau/Groupes)** et le chapitre « Objets pour le contrôle d'accès » du guide de configuration du pare-feu ASA pour en savoir plus sur les groupes d'objets réseau.

Le réseau IP sous-jacent entre les VTEP est indépendant du réseau de liaison de commande de grappe utilisé par les interfaces VNI (VXLAN Network Identifier). Chaque interface source de VTEP possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

Étape 2 Configurez l'interface source VTEP.

L'interface source du VTEP est une interface ASA virtuel classique à laquelle vous prévoyez associer l'interface VNI. Vous pouvez configurer une interface source de VTEP pour qu'elle agisse en tant que liaison de commande de grappe. L'interface source est réservée à une utilisation avec la liaison de commande de grappe uniquement.

a) Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, et modifiez l'interface que vous souhaitez utiliser pour l'interface source VTEP.
b) Configurez l'**Interface Name** (Nom de l'interface).
c) Cochez la case **VTEP Source Interface (cluster)** (Interface source VTEP (grappe)).
d) Cochez **Enable Interface** (Activer l'interface).
e) Configurez une adresse IPv4 statique.

   L'adresse IP doit être incluse comme l'un des homologues dans le groupe d'objets réseau.

f) Cliquez sur l'onglet **Advanced** (Avancé) et définissez la **MTU** de la liaison de commande de grappe pour être au moins 154 octets supérieure à la MTU la plus élevée des interfaces de données.

   Étant donné que le trafic de la liaison de commande de grappe comprend la transmission de paquets de données, celle-ci doit prendre en charge la taille totale d'un paquet de données, plus les surcharges de trafic de la grappe (100 octets) et les surcharges VXLAN (54 octets). Définissez la MTU entre 1 554 et 9 198 octets. Par défaut, la MTU est de 1554 octets. Nous vous conseillons de définir la MTU de liaison de commande de grappe à 1654 lorsque les interfaces de données sont fixées à 1500; cette valeur nécessite la réservation de bâti grand format, ce qui requiert un rechargement.

   Par exemple, lors de l'utilisation d'un bâti grand format, comme la MTU maximale est de 9 198 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9 044, tandis que la liaison de commande de grappe peut être définie sur 9 198.

g) Cliquez sur **OK**.

Étape 3 Associez l'interface source VTEP à l'instance du terminal de virtualisation du réseau (NVE).

a) Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **VXLAN** .
b) (Facultatif) Saisissez une valeur dans **VXLAN Destination Port** (Port de destination VXLAN) si vous souhaitez modifier la valeur par défaut de 4789.
c) Cochez la case **Enable Network Virtualization Endpoint encapsulation using VXLAN** (Activer l'encapsulation du terminal de virtualisation du réseau à l'aide de VXLAN).

d) Choisissez l'option **VTEP Tunnel Interface** (Interface de tunnel VTEP) dans la liste déroulante.
e) Cochez la case **Configure Packet Recipient** (Configurer le destinataire des paquets), cliquez sur le bouton radio **Peer Group** (Groupe d'homologues) et choisissez le groupe d'homologues que vous avez créé.
f) Cliquez sur **Apply** (Appliquer).

Étape 4 Créez l'interface VNI.

Une interface VNI est semblable à une interface VLAN : il s'agit d'une interface virtuelle qui sépare le trafic réseau sur une interface physique donnée au moyen de balisage. Vous ne pouvez configurer qu'une seule interface VNI.

a) Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres de l'interface)** > **Interfaces** et cliquez sur **Add (Ajouter)** > **VNI Interface (Interface VNI)**.
b) Saisissez le **VNI ID** (ID VNI) compris entre 1 et 10 000.

   Cet ID est simplement un identifiant d'interface interne.

c) Saisissez le **VNI Segment ID** (ID de segment VNI) compris entre 1 et 16777215.

   L'ID de segment est utilisé pour le balisage VXLAN.

d) Cochez la case **NVE Mapped to VTEP Interface** (NVE mappé à l'interface VTEP).

   Ce paramètre associe l'interface VNI à l'interface source VTEP.

e) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Configurer les interfaces individuelles

Vous devez modifier toute interface actuellement configurée avec une adresse IP pour qu'elle soit prête pour la grappe avant d'activer la mise en grappe. Au minimum, vous devrez peut-être modifier l'interface de gestion à laquelle ASDM est actuellement connecté lorsque vous utilisez une adresse IP statique pour la gestion. Pour les autres interfaces, vous pouvez les configurer avant ou après avoir activé la mise en grappe; nous vous conseillons de préconfigurer toutes vos interfaces afin que la configuration complète soit synchronisée avec les nouveaux nœuds de la grappe.

Cette section décrit comment configurer les interfaces pour qu'elles soient compatibles avec la mise en grappe. Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre adresse IP prise dans un ensemble d'adresses IP. L'adresse IP de la grappe principale est une adresse fixe pour la grappe qui appartient toujours au nœud de contrôle actuel. Toutes les interfaces de données doivent être des interfaces individuelles.

Pour l'interface de gestion, vous pouvez configurer un ensemble d'adresses IP ou utiliser le protocole DHCP; seule l'interface de gestion prend en charge l'obtention d'une adresse de DHCP. Pour utiliser DHCP, n'utilisez pas cette procédure; configurez-le plutôt comme d'habitude (voir Configurer les paramètres généraux de l'interface en mode routé, à la page 698).

Avant de commencer

- (Facultatif) Configurez les sous-interfaces.
- Pour l'interface de gestion, vous pouvez utiliser une adresse statique ou le protocole DHCP. Si vous utilisez des adresses IP statiques et que vous vous connectez à distance à l'interface de gestion à l'aide d'ASDM, l'adresse IP actuelle des nœuds de données potentiels est à usage temporaire.

- Une adresse IP sera attribuée à chaque membre dans l'ensemble d'adresses IP de la grappe défini sur le nœud de contrôle.
- L'ensemble d'adresses IP de la grappe ne peut pas inclure des adresses déjà utilisées sur le réseau, y compris de potentielles adresses IP secondaires.

  Par exemple :

  1. Vous configurez le nœud de contrôle pour qu'il utilise 10.1.1.1.
  2. Les autres nœuds utilisent 10.1.1.2, 10.1.1.3 et 10.1.1.4.
  3. Lorsque vous configurez l'ensemble d'adresses IP de la grappe sur le nœud de contrôle, vous ne pouvez pas inclure les adresses .2, .3 ou .4 dans l'ensemble, car elles sont déjà utilisées.
  4. Vous devez plutôt utiliser d'autres adresses IP sur le réseau, telles que .5, .6, .7 et .8.



Remarque L'ensemble a besoin d'autant d'adresses qu'il y a de membres dans la grappe, y compris le nœud de contrôle; l'adresse .1 d'origine est l'adresse IP principale de la grappe qui appartient au nœud de contrôle actuel.

5. Après avoir rejoint la grappe, les anciennes adresses temporaires sont abandonnées et peuvent être utilisées ailleurs.

Procédure

Étape 1 Choisissez le volet**Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.

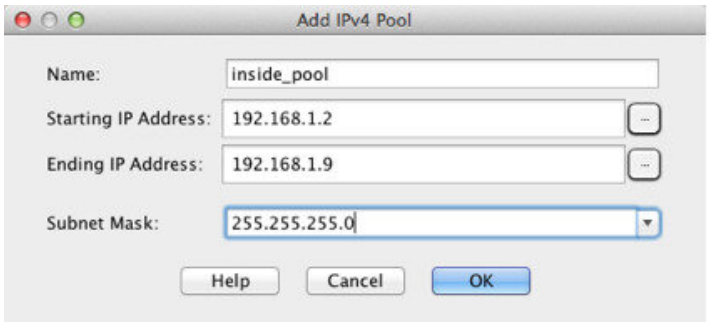
Étape 2 Choisissez la ligne d'interface, puis cliquez sur modifier (**Edit**). Choisissez **Use Static IP** (Utiliser l'adresse IP statique). Les protocoles DHCP et PPPoE ne sont pas pris en charge.

Étape 3 Pour ajouter l'ensemble d'adresses IP de la grappe IPv4, l'ensemble d'adresses MAC et les adresses MAC spécifiques au site, cliquez sur l'onglet **Advanced** (Avancé) et définissez les paramètres de la zone **ASA Cluster** (Grappe ASA).

a) Créez un ensemble d'adresses IP de grappe en cliquant sur le bouton **…** à côté du champ **IP Address Pool** (Ensemble d'adresses IP). La plage valide affichée est déterminée par l'adresse IP principale que vous avez définie dans l'onglet General (Général).

b) Cliquez sur **Add** (ajouter).

c) Configurez une plage d'adresses qui ne comprend pas l'adresse IP principale de la grappe et qui n'inclut aucune adresse actuellement utilisée sur votre réseau. Vous devez définir une plage suffisamment large pour la taille de la grappe, par exemple, 8 adresses.



d) Cliquez sur **OK** pour créer le nouvel ensemble.
e) Sélectionnez le nouvel ensemble que vous avez créé, cliquez sur **Assign** (Affecter), puis cliquez sur **OK**.

   Le nom de l'ensemble apparaît dans le champ **IP Address Pool** (Ensemble d'adresses IP).

f) (Facultatif) (Facultatif) Configurez un **MAC Address Pool** (Ensemble d'adresses MAC) si vous souhaitez configurer manuellement des adresses MAC.

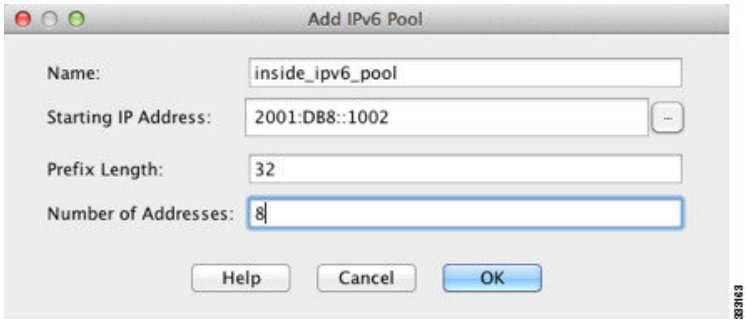
Étape 4 Pour configurer une adresse IPv6, cliquez sur l'onglet **IPv6**.

a) Cochez la case **Enable IPv6** (activer IPv6).
b) Dans la zone **Interface IPv6 Addresses** (Adresses IPv6 de l'interface), cliquez sur **Add** (Ajouter).

   L'option **Enable address autoconfiguration** (Activer l'autoconfiguration de l'adresse) n'est pas prise en charge. La configuration manuelle de l'adresse Link-Local n'est pas non plus prise en charge.

   La boîte de dialogue **Add IPv6 Address for Interface** (ajouter une adresse IPv6 pour l'interface) s'affiche.

c) Dans le champ **Address/Prefix Length** (Longueur d'adresse/préfixe), saisissez l'adresse IPv6 globale et la longueur du préfixe IPv6. Par exemple : 2001:0DB8::BA98:0:3210/48.
d) Cliquez sur le bouton **...** pour configurer l'ensemble d'adresses IP de la grappe.
e) Cliquez sur **Add** (ajouter).



f) Configurez l'adresse IP de départ (préfixe de réseau), la longueur du préfixe et le nombre d'adresses dans le groupe d'adresses.
g) Cliquez sur **OK** pour créer le nouvel ensemble.
h) Sélectionnez le nouvel ensemble que vous avez créé, cliquez sur **Assign** (Affecter), puis cliquez sur **OK**.

   Le groupe apparaît dans le champ **ASA Cluster IP Pool** (Ensemble d'adresses IP de grappe ASA).

i) Cliquez sur **OK**.

Étape 5 Cliquez sur **OK** pour revenir au volet Interfaces.

Étape 6 Cliquez sur **Apply** (Appliquer).

Créer ou joindre une grappe à l'aide de l'assistant de haute disponibilité

Chaque nœud de la grappe nécessite une configuration de démarrage pour rejoindre la grappe. Exécutez l'assistant de haute disponibilité et évolutivité sur un nœud (qui deviendra le nœud de contrôle) pour créer la grappe, puis ajoutez-y des nœuds de données.

Avant de commencer

- L'interface source VXLAN VTEP que vous comptez utiliser pour l'interface de liaison de commande de grappe doit être à l'état activée sur le commutateur connecté.
- Lorsque vous ajoutez un nœud à une grappe en cours d'exécution, il se peut que vous constatiez des interruptions temporaires et limitées de paquets/connexions; c'est un comportement prévu.

Procédure

Étape 1 Choisissez **Wizards (Assistants)** > **High Availability and Scalability Wizard (Assistant de haute disponibilité et d'évolutivité)**. Consultez les instructions relatives à l'assistant dans les étapes suivantes.

Étape 2 Dans l'écran ASA Cluster Configuration (Configuration de la grappe ASA), configurez les paramètres de démarrage, notamment :

- **Member Priority (Priorité des membres)**— Définit la priorité de ce nœud pour les élections du nœud de contrôle, entre 1 et 100, où 1 est la priorité la plus élevée.
- **Site Index** (Index du site) : si vous utilisez la mise en grappe inter-sites, définissez l'ID de site pour ce nœud afin qu'il utilise une adresse MAC spécifique au site, entre 1 et 8.
- (Facultatif) **Shared Key (Clé partagée)** : Définit une clé de chiffrement pour le trafic de contrôle sur la liaison de commande de grappe. Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères. Le secret partagé est utilisé pour générer la clé de chiffrement. Ce paramètre n'influe pas sur le trafic datapath, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair. Vous devez configurer ce paramètre si vous activez également le service de chiffrement du mot de passe.
- (Facultatif) **Enable connection rebalancing for TCP traffic across all the ASAs in the cluster (Activer le rééquilibrage de connexion pour le trafic TCP sur tous les ASA de la grappe)** : permet de rééquilibrer la connexion. Le paramètre par défaut de ce filtre est désactivé. Si cette option est activée, les ASA d'une grappe échangent périodiquement des informations de chargement et déchargent les nouvelles connexions des appareils plus chargés vers les appareils moins chargés. La fréquence, comprise entre 1 et 360 secondes, spécifie la fréquence à laquelle les informations de chargement sont échangées. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données.

Remarque Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

- (Facultatif) **Enable health monitoring of this device within the cluster** (Activer la surveillance de l'intégrité de ce périphérique au sein de la grappe) : active la fonction de vérification de l'intégrité des nœuds de la grappe. Pour déterminer l'intégrité des nœuds, les nœuds de la grappe ASA envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.

Remarque Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que le changement de configuration est synchronisé avec tous les nœuds, vous pouvez réactiver le contrôle de l'intégrité.

  - **Time to Wait Before Device Considered Failed** (Temps d'attente avant que l'appareil ne soit reconnu comme défaillant) : cette valeur détermine la durée entre les messages d'état keepalive du nœud, entre 0,3 et 45 secondes; la valeur par défaut est de 3 secondes.

- (Facultatif) **Replicate console output** (Répliquer l'extrant de la console) : permet la réplication de la console des nœuds de données vers le nœud de contrôle. Par défaut, cette fonction est désactivée. L'ASA peut imprimer certains messages directement sur la console pour certains événements critiques. Si vous activez la réplication de la console, les nœuds de données envoient les messages de la console au nœud de contrôle de sorte que vous ne devez surveiller qu'un seul port de console pour la grappe. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données.
- **Cluster Control Link** (Liaison de commande de grappe) : spécifie l'interface de liaison de commande de grappe.
  - **MTU** : spécifiez l'unité de transfert maximale de l'interface source VTEP, qui doit être supérieure d'au moins 154 octets à la MTU la plus élevée des interfaces de données. Étant donné que le trafic de la liaison de commande de grappe comprend la transmission de paquets de données, celle-ci doit prendre en charge la taille totale d'un paquet de données, plus les surcharges de trafic de la grappe (100 octets) et les surcharges VXLAN (54 octets). Définissez la MTU entre 1 554 et 9 198 octets. Par défaut, la MTU est de 1554 octets. Nous vous suggérons de définir la MTU de liaison de commande de grappe à 1 654 lorsque les interfaces de données sont définies à 1 500; cette valeur nécessite la réservation de bâti grand format. Par exemple, lors de l'utilisation d'un bâti grand format, comme la MTU maximale est de 9 198 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9 044, tandis que la liaison de commande de grappe peut être définie sur 9 198. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données. **Remarque :** Si vous n'avez pas de réservation de trame étendue pré-activée, vous devez quitter l'assistant, activer les trames étendues, puis relancer cette procédure.

Étape 3 Sur l'écran **Interfaces for Health Monitoring** (Interfaces de contrôle d'intégrité), vous pouvez exempter certaines interfaces de la surveillance en cas d'échec. Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion.

Remarque Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que le changement de configuration est synchronisé avec tous les nœuds, vous pouvez réactiver le contrôle de l'intégrité.

Étape 4 Dans l'écran **Interface Auto Rejoin settings** (Paramètres de la jonction automatique de l'interface), personnalisez les paramètres de la jonction automatique en cas de défaillance de l'interface ou de la liaison de commande de grappe. Pour chaque type, vous pouvez définir les paramètres suivants :

- **Maximum Rejoin Attempts** (Nombre maximal de tentatives de jonction) : Permet de définir le nombre de tentatives de jonction à la grappe en sélectionnant **Unlimited** (Illimité) ou une valeur comprise entre 0 et 65 535. **0** désactive la jonction automatique. La valeur par défaut est **Unlimited** (Illimité) pour l'interface de grappe et **3** pour l'interface de données.
- **Rejoin Interval** (Intervalle de jonction) : permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est **5** minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente en définissant la variation d'intervalle entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente) ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l'interface de grappe et **2** pour l'interface de données.

Étape 5 Cliquez sur **Finish** (Terminer).

Étape 6 L'ASA analyse la configuration en cours à la recherche de commandes incompatibles, en vue de cerner des fonctionnalités qui ne sont pas prises en charge avec la grappe, y compris les commandes pouvant être présentes dans la configuration par défaut. Cliquez sur **OK** pour supprimer les commandes incompatibles. Si vous cliquez sur **Cancel** (annuler), la mise en grappe n'est pas activée.

Après un certain temps, pendant qu'ASDM active la mise en grappe et se reconnecte à l'ASA, l'écran d'information apparaît pour confirmer que l'ASA a été ajouté à la grappe.

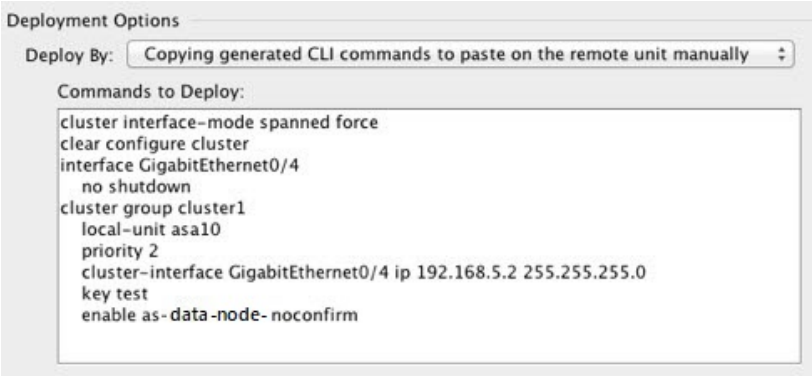
Remarque Dans certains cas, il se peut qu'une erreur se produise lors de la connexion à la grappe, une fois que le processus de l'assistant est terminé. Si ASDM a été déconnecté, ASDM ne recevra aucune erreur subséquente de l'ASA. Si la mise en grappe demeure désactivée après la reconnexion d'ASDM, vous devez vous connecter au port de console d'ASA pour déterminer la condition d'erreur exacte qui a désactivé la mise en grappe; par exemple, la liaison de commande de grappe peut être inactive.

Étape 7 Pour ajouter un nœud de données, cliquez sur **Yes (oui)**.

Si vous réexécutez l'assistant à partir du nœud de contrôle, vous pouvez ajouter des nœuds de données en choisissant l'option **Add another member to the cluster (ajouter un autre membre à la grappe)** lorsque vous lancez l'assistant pour la première fois.

Étape 8 Dans la zone des options de déploiement (**Deployment Options**), choisissez l'une des options suivantes (**Deploy By**) :

- **Envoi de commandes de l'interface de ligne de commande à l'unité distante maintenant—** Envoi de la configuration de démarrage à l'adresse IP de gestion du nœud de données (temporaire). Saisissez l'adresse IP de gestion du nœud de données, le nom d'utilisateur et le mot de passe.
- **Copie des commandes de l'interface de ligne de commande générées pour les coller manuellement sur l'unité distante**— génère les commandes afin que vous puissiez les couper et les coller sur l'interface de commande du nœud de données ou à l'aide de l'outil de l'interface de ligne de commande dans ASDM. Dans la zone des commandes à déployer, sélectionnez et copiez les commandes générées pour une utilisation ultérieure.



Personnaliser l'opération de mise en grappe

Vous pouvez personnaliser la surveillance de l'intégrité de la mise en grappe, le délai de réplication de la connexion TCP, la mobilité des flux et d'autres optimisations, dans le cadre de la configuration day0 ou après le déploiement de la grappe.

Exécutez ces procédures sur le nœud de contrôle.

Configurer les paramètres de grappe ASA de base

Vous pouvez personnaliser les paramètres de grappe sur le nœud de contrôle. Si vous n'utilisez pas l'assistant pour ajouter un nœud à la grappe, vous pouvez configurer les paramètres de grappe manuellement. Si vous avez déjà activé la mise en grappe, vous pouvez modifier certains paramètres de grappe; d'autres qui ne peuvent pas être modifiés lorsque la mise en grappe est activée sont grisés. Cette procédure inclut également les paramètres avancés qui ne sont pas inclus dans l'assistant.

Avant de commencer

- Si vous n'avez pas utilisé l'assistant et que vous souhaitez joindre manuellement la grappe, vous devez préconfigurer la liaison de commande de grappe sur chaque nœud avant de joindre la grappe. Consultez Configurer la liaison de commande de grappe sur le nœud de contrôle, à la page 563.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**.

Si votre périphérique est déjà dans la grappe et qu'il s'agit du nœud de contrôle, ce volet se trouve dans l'onglet **Cluster Configuration** (Configuration de la grappe).

Étape 2 Cochez la case **Configure ASA cluster settings** (Configurer les paramètres de grappe ASA).

Si vous décochez la case, les paramètres sont effacés. Ne cochez pas **Participate in ASA cluster** (Participer à la grappe ASA) avant d'avoir défini tous vos paramètres.

Remarque Après avoir activé la mise en grappe, ne décochez pas la case **Configure ASA cluster settings** (Configurer les paramètres de grappe ASA) sans comprendre les conséquences. Cette action efface toute la configuration de la grappe et désactive également toutes les interfaces, y compris l'interface de gestion à laquelle ASDM est connecté. Pour rétablir la connectivité dans ce cas, vous devez accéder à l'interface de ligne de commande au niveau du port de console.

Étape 3 Configurez les paramètres de démarrage suivants :

- **Cluster Name** (Nom de la grappe) : nomme la grappe. Le nom doit être une chaîne ASCII comptant de 1 à 38 caractères. Vous ne pouvez configurer qu'une seule grappe par nœud. Tous les membres de la grappe doivent utiliser le même nom.
- **Member Name** (Nom de membre) : nomme ce membre de la grappe avec une chaîne ASCII unique de 1 à 38 caractères.
- **Member Priority** (Priorité des membres) : définit la priorité de ce nœud pour les élections du nœud de contrôle, entre 1 et 100, où 1 est la priorité la plus élevée.
- **Site Index** (Index du site) : si vous utilisez la mise en grappe inter-sites, définissez l'ID de site pour ce nœud afin qu'il utilise une adresse MAC spécifique au site, entre 1 et 8.
- (Facultatif) **Shared Key** (Clé partagée) : définit une clé de chiffrement pour le trafic de contrôle sur la liaison de commande de grappe. Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères. Le secret partagé est utilisé pour générer la clé de chiffrement. Ce paramètre n'influe pas sur le trafic datapath, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair. Vous devez configurer ce paramètre si vous activez également le service de chiffrement du mot de passe.
- (Facultatif) **Enable connection rebalancing for TCP traffic across all the ASAs in the cluster (Activer le rééquilibrage de connexion pour le trafic TCP sur tous les ASA de la grappe)** : permet de rééquilibrer la connexion. Le paramètre par défaut de ce filtre est désactivé. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données. Si

cette option est activée, les ASA échangent périodiquement des renseignements sur les connexions par seconde et déchargent les nouvelles connexions des appareils ayant plus de connexions par seconde vers les appareils moins chargés. Les connexions existantes ne sont jamais déplacées. De plus, comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal. La fréquence, comprise entre 1 et 360 secondes, spécifie la fréquence à laquelle les informations de chargement sont échangées. La valeur par défaut est de 5 secondes.

Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

- **Enable cluster load monitor** (Activer le moniteur de charge de la grappe) : vous pouvez superviser la charge de trafic pour les membres de la grappe, y compris le nombre total de connexions, l'utilisation du CPU et de la mémoire, ainsi que les abandons de tampon. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur le nœud si les nœuds restants peuvent gérer la charge ou de régler l'équilibrage de charges sur le commutateur externe. Cette fonction est activée par défaut. Vous pouvez superviser périodiquement la charge de trafic. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur le nœud.

  Définissez les paramètres suivants :

  - **Time Interval** (Intervalle de temps) : définit le temps en secondes entre les messages de supervision, entre 10 et 360 secondes. La valeur par défaut est de 20 secondes.
  - **Number of Intervals** (Nombre d'intervalles) : définit le nombre d'intervalles pour lesquels l'ASA conserve les données, entre 1 et 60. La valeur par défaut est 30.

  Consultez **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Load-Monitoring (Supervision de la charge de la grappe)** pour afficher la charge de trafic.

- (Facultatif) **Enable health monitoring of this device within the cluster** (Activer la surveillance de l'intégrité de ce périphérique dans la grappe) : active la fonctionnalité de vérification de l'intégrité des nœuds de la grappe et détermine le temps entre les messages d'état de pulsation des nœuds, entre 0,3 et 45 secondes; la valeur par défaut est de 3 secondes. **Remarque** : lorsque vous ajoutez de nouveaux nœuds à la grappe et apportez des modifications de topologie à l'ASA ou au commutateur, vous devez désactiver temporairement cette fonctionnalité jusqu'à ce que la grappe soit terminée et désactiver la supervision d'interface pour les interfaces désactivées (**Configuration** > **Device Management [Gestion des périphériques]** > **High Availability and Scalability [Haute disponibilité et évolutivité]** > **ASA Cluster [Grappe ASA]** > **Cluster Interface Health Monitoring [Surveillance de l'intégrité de l'interface de grappe]**). Vous pouvez réactiver cette fonctionnalité une fois les modifications apportées à la grappe et à la topologie terminées. Pour déterminer l'intégrité des nœuds, les nœuds de la grappe ASA envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.

- (Facultatif) **Debounce Time** (Délai antirebond) : configure le délai antirebond avant que l'ASA considère une interface comme défaillante et que le nœud ne soit supprimé de la grappe. Cette fonctionnalité permet une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Le délai antirebond par défaut est de 500 ms, avec une plage de 300 ms à 9 secondes.

- (Facultatif) **Replicate console output** (Répliquer l'extrant de la console) : permet la réplication de la console des nœuds de données vers le nœud de contrôle. Par défaut, cette fonction est désactivée. L'ASA peut imprimer certains messages directement sur la console pour certains événements critiques. Si vous activez la réplication de la console, les nœuds de données envoient les messages de la console au nœud de contrôle de sorte que vous ne devez surveiller qu'un seul port de console pour la grappe. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données.
- (Facultatif) **Enable Clustering Flow Mobility** (Activer la mobilité des flux de grappes). Consultez Configurer l'inspection LISP, à la page 579.
- (Facultatif) **Enable Director Localization for inter-DC cluster** (Activer la localisation de directeur pour la grappe inter-DC) : pour améliorer les performances et réduire la latence d'aller-retour dans le cas de la mise en grappe inter-sites pour les centres de données, vous pouvez activer la localisation de directeur. Les nouvelles connexions sont généralement équilibrées et appartiennent aux membres de la grappe d'un site donné. Cependant, l'ASA attribue le rôle de directeur à un membre sur *n'importe quel* site. La localisation du directeur permet des rôles de directeur supplémentaires : un directeur local sur le même site que le propriétaire et un directeur global qui peut se trouver sur n'importe quel site. Le fait de garder le propriétaire et le directeur sur le même site améliore les performances. De plus, en cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site. Le directeur global est utilisé si un membre d'une grappe reçoit des paquets pour une connexion appartenant à un autre site.
- (Facultatif) **Site Redundancy** (Redondance de site) : pour protéger les flux contre une défaillance de site, vous pouvez activer la redondance de site. Si le propriétaire de connexion de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La localisation de directeur et la redondance de site sont des fonctionnalités distinctes; vous pouvez configurer l'un ou l'autre, ou configurer les deux.
- (Facultatif) **Enable config sync acceleration** (Activer l'accélération de la synchronisation de la configuration) : lorsqu'un nœud de données a la même configuration que le nœud de contrôle, il ignorera la synchronisation de la configuration et se joindra plus rapidement. Cette fonction est activée par défaut. Cette fonctionnalité est configurée sur chaque nœud et n'est pas répliquée du nœud de contrôle au nœud de données.

Remarque Certaines commandes de configuration ne sont pas compatibles avec la jonction accélérée de grappes; si ces commandes sont présentes sur le nœud, même si la jonction accélérée de grappes est activée, la synchronisation de la configuration se produira toujours. Vous devez supprimer la configuration incompatible pour que la jonction accélérée de grappes fonctionne. Utilisez la commande **show cluster info unit-join-acceleration incompatible-config** pour afficher la configuration incompatible.

- **Enable parallel configuration replicate** (Activer la réplication de configuration parallèle) : permet au nœud de contrôle de synchroniser les modifications de configuration avec les nœuds de données en parallèle. Sinon, la synchronisation a lieu de manière séquentielle et peut prendre plus de temps.
- **Cluster Control Link** (Liaison de commande de grappe) : spécifie l'interface de liaison de commande de grappe.
  - **Interface** : spécifie l'interface VNI.

- **IP Address** (Adresse IP) : spécifie une adresse IPv4 pour l'adresse IP; IPv6 n'est pas pris en charge pour cette interface.
- **Subnet Mask** (Filtre d'adresse locale) : spécifie le filtre d'adresse locale.
- **MTU** : spécifie l'unité de transfert maximale de l'interface source VTEP, qui doit être supérieure d'au moins 154 octets à la MTU la plus élevée des interfaces de données. Étant donné que le trafic de la liaison de commande de grappe comprend la transmission de paquets de données, celle-ci doit prendre en charge la taille totale d'un paquet de données, plus les surcharges de trafic de la grappe (100 octets) et les surcharges VXLAN (54 octets). Définissez la MTU entre 1 554 et 9 198 octets. Par défaut, la MTU est de 1554 octets. Nous vous suggérons de définir la MTU de liaison de commande de grappe à 1 654 lorsque les interfaces de données sont définies à 1 500; cette valeur nécessite la réservation de bâti grand format. Par exemple, lors de l'utilisation d'un bâti grand format, comme la MTU maximale est de 9 198 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9 044, tandis que la liaison de commande de grappe peut être définie sur 9 198. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données.

  Remarque : si vous n'avez pas activé au préalable la réservation de bâti grand format, activez les bâtis grand format, puis recommencez cette procédure.

Étape 4 Cochez la case **Participate in ASA cluster** (Participer à la grappe ASA) pour rejoindre la grappe.

Étape 5 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de surveillance de l'intégrité de l'interface et de jonction automatique

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Interface Health Monitoring (Surveillance de l'intégrité de l'interface de grappe)**.

Étape 2 Dans la zone **Monitored Interfaces** (Interfaces surveillées), sélectionnez une interface et cliquez sur **Add** (Ajouter) pour la déplacer vers la zone **Unmonitored Interfaces** (Interfaces non surveillées).

Les messages d'état de l'interface détectent une défaillance de liaison. Si un nœud ne reçoit pas de messages d'état d'interface dans le délai de rétention, le temps avant que l'ASA ne supprime un membre de la grappe dépend du fait que le nœud soit un membre établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces.

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur), vous devez désactiver le contrôle d'intégrité (**Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**) et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver le contrôle d'intégrité.

Étape 3 Cliquez sur l'onglet **Auto Rejoin** (Jonction automatique) pour personnaliser les paramètres de la jonction automatique en cas de défaillance de l'interface, du système ou de la liaison de commande de grappe. Pour chaque type, cliquez sur **Edit** (Modifier) pour définir les éléments suivants :

- **Maximum Rejoin Attempts** (Nombre maximal de tentatives de jonction) : Permet de définir le nombre de tentatives de jonction à la grappe en sélectionnant **Unlimited** (Illimité) ou une valeur comprise entre 0 et 65 535. **0** désactive la jonction automatique. La valeur par défaut est **Unlimited** (Illimité) pour l'interface de grappe et **3** pour l'interface de données et le système.
- **Rejoin Interval** (Intervalle de jonction) : permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est **5** minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente en définissant la variation d'intervalle entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente) ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l'interface de grappe et **2** pour l'interface de données et le système.

Cliquez sur **Restore Defaults** pour rétablir les paramètres par défaut.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer le délai de réplication TCP de la grappe

Activez le délai de réplication de la grappe pour les connexions TCP pour aider à éliminer le « travail inutile » lié aux flux de courte durée en retardant la création du flux directeur/de sauvegarde. Notez que si une unité tombe en panne avant la création du flux directeur/de sauvegarde, ces flux ne peuvent pas être récupérés. De même, si le trafic est rééquilibré vers une autre unité avant la création du flux, le flux ne peut pas être récupéré. Vous ne devez pas activer la réplication TCP pour le trafic sur lequel vous désactivez la répartition aléatoire TCP.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster Replication (Réplication de la grappe ASA)**.

Étape 2 Cliquez sur **Add** (Ajouter) et réglez les valeurs suivantes :

- **Replication delay** (Délai de réplication) : définissez les secondes entre 1 et 15.
- **HTTP** : définissez le délai pour tout le trafic HTTP.
- **Critères de source**
  - **Source** : définissez l'adresse IP source.
  - **Service** : (Facultatif) Définissez le port source. En général, vous définissez soit le port source, soit le port de destination, mais pas les deux.
- **Critères de destination**
  - **Source** : définissez l'adresse IP de destination.
  - **Service** : (Facultatif) Définissez le port de destination. En général, vous définissez soit le port source, soit le port de destination, mais pas les deux.

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer les fonctionnalités inter-sites

Pour la mise en grappe inter-sites, vous pouvez personnaliser votre configuration pour améliorer la redondance et la stabilité.

Configurer la mobilité des flux de grappes

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

À propos de l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux entre les sites.

À propos de LISP

La mobilité des machines virtuelles de centres de données, comme VMware VMotion, permet aux serveurs de migrer entre les centres de données tout en maintenant les connexions avec les clients. Pour prendre en charge une telle mobilité de serveur de centre de données, les routeurs doivent être en mesure de mettre à jour la route d'entrée vers le serveur lorsqu'il se déplace. L'architecture Cisco Locator/Protocole de séparation d'ID (LISP) sépare l'identité du périphérique, ou l'identifiant de terminal (EID), de son emplacement, ou localisateur de routage, dans deux espaces de numérotation différents, ce qui rend la migration du serveur transparente pour les clients. Par exemple, lorsqu'un serveur est déplacé vers un nouveau site et qu'un client envoie du trafic vers le serveur, le routeur redirige le trafic vers le nouvel emplacement.

LISP nécessite des routeurs et des serveurs dans certains rôles, tels que le routeur de tunnel de sortie (ETR) LISP, le routeur de tunnel d'entrée (ITR), les routeurs de premier saut, le résolveur de carte (MR) et le serveur de carte (MS). Lorsque le routeur du premier saut du serveur détecte que le serveur est connecté à un autre routeur, il met à jour tous les autres routeurs et les bases de données afin que l'ITR connectée au client puisse intercepter, encapsuler et envoyer le trafic vers le nouvel emplacement du serveur.

Prise en charge du LISP ASA

L'ASA n'exécute pas le LISP lui-même; il peut, cependant, inspecter le trafic LISP pour détecter les changements d'emplacement, puis utiliser ces informations pour un fonctionnement de mise en grappe transparent. Sans l'intégration du LISP, lorsqu'un serveur est déplacé vers un nouveau site, le trafic est acheminé vers un membre de la grappe ASA sur le nouveau site plutôt que vers le propriétaire d'origine du flux. Le nouvel ASA transfère le trafic vers l'ASA au niveau de l'ancien site, puis l'ancien ASA doit renvoyer le trafic vers le nouveau site pour qu'il atteigne le serveur. Ce flux de trafic est sous-optimal et est connu comme « tromboning » ou « épingle à cheveux ».

Grâce à l'intégration du LISP, les membres de la grappe ASA peuvent inspecter le trafic LISP passant entre le routeur du premier saut et l'ETR ou l'ITR, puis peuvent changer le propriétaire du flux pour qu'il se trouve sur le nouveau site.

Lignes directrices LISP

- Les membres de la grappe ASA doivent se trouver entre le routeur du premier saut et l'ITR ou l'ETR du site. La grappe ASA elle-même ne peut pas être le premier routeur de saut pour un segment étendu.
- Seuls les flux entièrement distribués sont pris en charge; les flux centralisés, les flux semi-distribués ou les flux appartenant à des nœuds individuels ne sont pas transférés vers de nouveaux propriétaires. Les flux semi-distribués comprennent des applications, telles que SIP, où tous les flux enfants appartiennent au même ASA qui possède le flux parent.
- La grappe déplace uniquement les états de flux de couche 3 et 4; certaines données d'application pourraient être perdues.
- Pour les flux de courte durée ou non essentiels pour l'entreprise, le déplacement du propriétaire peut ne pas valoir la peine. Vous pouvez contrôler les types de trafic pris en charge avec cette fonctionnalité lorsque vous configurez la politique d'inspection. Vous devez limiter la mobilité de flux au trafic essentiel.

Mise en œuvre du LISP ASA

Cette fonctionnalité comprend plusieurs configurations interdépendantes (qui sont toutes décrites dans ce chapitre) :

1. (Facultatif) Limiter les EID inspectés en fonction de l'adresse IP de l'hôte ou du serveur : le routeur de premier saut pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée, vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.
2. Inspection du trafic LISP : l'ASA inspecte le trafic LISP sur le port UDP 4342 pour détecter le message EID-notify envoyé entre le premier saut du routeur et l'ITR ou l'ETR. L'ASA gère un tableau EID qui met en corrélation l'EID et l'ID de site. Par exemple, vous devez inspecter le trafic LISP avec une adresse IP source du routeur du premier saut et une adresse de destination de l'ITR ou de l'ETR. Remarque : le trafic LISP n'a pas de directeur affecté et le trafic LISP en lui-même ne participe pas au partage de l'état de la grappe.
3. Politique de service pour activer la mobilité des flux sur le trafic spécifié : vous devez activer la mobilité des flux sur le trafic critique. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques.
4. ID de sites : l'ASA utilise l'ID de site pour chaque nœud de la grappe afin de déterminer le nouveau propriétaire.

5. Configuration au niveau de la grappe pour activer la mobilité de flux : vous devez également activer la mobilité de flux au niveau de la grappe. Ce bouton bascule marche/arrêt vous permet d'activer ou de désactiver facilement la mobilité de flux pour une classe particulière de trafic ou d'applications.

Configurer l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

Avant de commencer

- Affectez chaque unité de grappe à un ID de site en fonction de Configurer les paramètres de grappe ASA de base, à la page 571.
- Le trafic LISP n'est pas inclus dans la classe de trafic d'inspection par défaut. Vous devez donc configurer une classe distincte pour le trafic LISP dans le cadre de cette procédure.

Procédure

Étape 1 (Facultatif) Configurez une carte d'inspection LISP pour limiter les EID inspectés en fonction de l'adresse IP et pour configurer la clé partagée LISP :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **LISP**.
b) Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
c) Saisissez un nom (40 caractères maximum) et une description.
d) Pour la commande **Allowed-EID access-list**, cliquez sur **Manage** (Gérer).

Le **gestionnaire ACL** s'ouvre.

Le routeur de premier saut ou l'ITR/ETR pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée; vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.

e) Ajoutez une ACL avec au moins un ACE en fonction du guide de configuration du pare-feu.
f) Si nécessaire, saisissez la **Validation Key** (Clé de validation).

Si vous avez copié une clé chiffrée, cliquez sur le bouton radio **Encrypted** (Chiffré).

g) Cliquez sur **OK**.

Étape 2 Ajoutez une règle de politique de service pour configurer l'inspection LISP :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.
b) Cliquez sur **Add** (ajouter).
c) Dans la page **Service Policy** (Politique de service), appliquez la règle à une interface ou globalement.

Si vous avez une politique de service existante que vous souhaitez utiliser, ajoutez une règle à cette politique. Par défaut, l'ASA comprend une politique globale appelée **global_policy**. Vous pouvez également créer une politique de service par interface si vous ne souhaitez pas appliquer la politique à l'échelle mondiale. L'inspection LISP est appliquée au trafic de manière bidirectionnelle, vous n'avez donc pas besoin d'appliquer la politique de service sur les interfaces source et de destination; tout le

trafic qui entre ou sort de l'interface à laquelle vous appliquez la règle est affecté si le trafic correspond à la carte dans les deux sens.

d) Sur la page **Traffic Classification Criteria** (Critères de classification du trafic), cliquez sur **Create a new traffic class** (Créer une nouvelle classe de trafic), et sous **Traffic Match Criteria** (Critères de correspondance du trafic), cochez la case **Source and Destination IP Address (uses ACL)** (Adresse IP source et de destination (utilise ACL)).

e) Cliquez sur **Next** (suivant).

f) Spécifiez le trafic que vous souhaitez inspecter. Vous devez spécifier le trafic entre le routeur de premier saut et l'ITR ou l'ETR sur le port UDP 4342. Les ACL IPv4 et IPv6 sont acceptées.

g) Cliquez sur **Next** (suivant).

h) Sur la page ou l'onglet de l'assistant **Rule Actions** (Actions de règles), sélectionnez l'onglet **Protocol Inspection** (Inspection du protocole).

i) Cochez la case **LISP**.

j) (Facultatif) Cliquez sur **Configure** (Configurer) pour choisir la carte d'inspection que vous avez créée.

k) Cliquez sur **Finish** (Terminer) pour enregistrer la règle de politique de service.

Étape 3 Ajoutez une règle de politique de service pour activer la mobilité des flux pour le trafic critique :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.

b) Cliquez sur **Add** (ajouter).

c) Sur la page **Service Policy** (Politique de service), choisissez la même politique de service que vous avez utilisée pour l'inspection LISP.

d) Sur la page **Traffic Classification Criteria** (Critères de classification du trafic), cliquez sur **Create a new traffic class** (Créer une nouvelle classe de trafic), et sous **Traffic Match Criteria** (Critères de correspondance du trafic), cochez la case **Source and Destination IP Address (uses ACL)** (Adresse IP source et de destination (utilise ACL)).

e) Cliquez sur **Next** (suivant).

f) Spécifiez le trafic opérationnel critique que vous souhaitez réaffecter au site le plus optimal lorsque les serveurs changent de site. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques. Les ACL IPv4 et IPv6 sont acceptées.

g) Cliquez sur **Next** (suivant).

h) Sur la page ou l'onglet de l'assistant **Rule Actions** (Actions de règles), sélectionnez l'onglet **Cluster** (Grappe).

i) Cochez la case **Enable Cluster flow-mobility triggered by LISP EID messages** (Activer la mobilité des flux de grappe déclenchée par les messages LISP EID).

j) Cliquez sur **Finish** (Terminer) pour enregistrer la règle de politique de service.

Étape 4 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)** > **et cochez la case Enable Clustering flow mobility** (Activer la mobilité des flux de la grappe).

Étape 5 Cliquez sur **Apply** (Appliquer).

Gérer les nœuds de la grappe

Après avoir déployé la grappe, vous pouvez modifier la configuration et gérer les nœuds de cette dernière.

Ajouter un nouveau nœud de données à partir du nœud de contrôle

Vous pouvez ajouter des nœuds de données supplémentaires à la grappe à partir du nœud de contrôle. Vous pouvez également ajouter des nœuds de données à l'aide de l'assistant de haute disponibilité et d'évolutivité. L'ajout d'un nœud de données à partir du nœud de contrôle a l'avantage de configurer la liaison de commande de grappe et de définir le mode d'interface de grappe sur chaque nœud de données que vous ajoutez.

Vous pouvez également vous connecter au nœud de données et configurer la mise en grappe directement sur ce dernier. Cependant, après avoir activé la mise en grappe, votre session ASDM sera déconnectée et vous devrez vous reconnecter.

Avant de commencer

- Si vous souhaitez envoyer la configuration de démarrage sur le réseau de gestion, assurez-vous que le nœud de données a une adresse IP accessible.

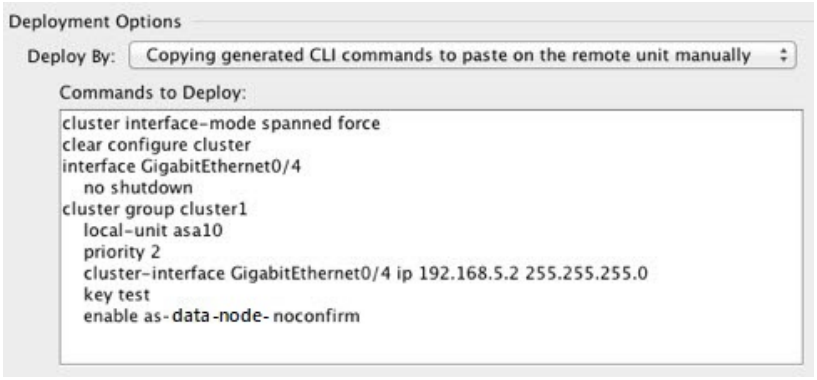
Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Members (Membres de la grappe)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Configurez selon les paramètres suivants :

- **Member Name** (Nom de membre) : nomme ce membre de la grappe avec une chaîne ASCII unique de 1 à 38 caractères.
- **Member Priority** (Priorité des membres) : définit la priorité de ce nœud pour les élections du nœud de contrôle, entre 1 et 100, où 1 est la priorité la plus élevée.
- **Cluster Control Link > IP Address** (Liaison de commande de grappe > Adresse IP) : spécifie une adresse IP unique pour ce membre pour la liaison de commande de grappe, sur le même réseau que la liaison de commande de grappe du nœud de contrôle.
- Dans la zone **Deployment Options** (Options de déploiement), choisissez l'une des options **Deploy By** (Déployer par) suivantes :
  - **Sending CLI commands to the remote unit now** (Envoi des commandes de l'interface de ligne de commande vers l'unité distante maintenant) : permet d'envoyer la configuration de démarrage à l'adresse IP de gestion (temporaire) de l'unité de données. Saisissez l'adresse IP de gestion du nœud de données, le nom d'utilisateur et le mot de passe.
  - **Copie des commandes de l'interface de ligne de commande générées pour les coller manuellement sur l'unité distante**— génère les commandes afin que vous puissiez les couper et les coller sur l'interface de commande du nœud de données ou à l'aide de l'outil de l'interface de ligne de commande dans ASDM. Dans la zone des commandes à déployer, sélectionnez et copiez les commandes générées pour une utilisation ultérieure.



Étape 4 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Devenir un nœud inactif

Pour devenir un membre inactif de la grappe, désactivez la mise en grappe sur le nœud tout en laissant intacte la configuration de mise en grappe.

Remarque Lorsqu'un ASA devient inactif (soit manuellement, soit à la suite d'un échec du contrôle d'intégrité), toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe; ou vous pouvez supprimer complètement le nœud de la grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), alors l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)**.

Étape 2 Décochez la case **Participer à la grappe ASA**.

Remarque Ne décochez pas la case **Configurer les paramètres de grappe ASA**. Cette action efface toute la configuration de la grappe et désactive également toutes les interfaces, y compris l'interface de gestion à laquelle ASDM est connecté. Pour rétablir la connectivité dans ce cas, vous devez accéder à l'interface de ligne de commande au niveau du port de console.

Étape 3 Cliquez sur **Apply** (Appliquer).

Désactiver un nœud de données à partir du nœud de contrôle

Pour désactiver un nœud de données, procédez comme suit.

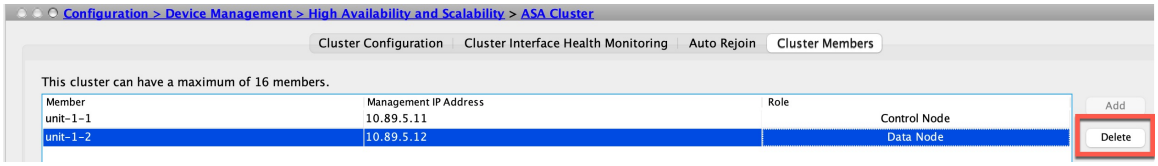
Remarque Lorsqu'un ASA devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Members (Membres de la grappe)**.

Étape 2 Sélectionnez le nœud de données que vous souhaitez supprimer et cliquez sur **Delete** (Supprimer).

Illustration 67 : Supprimer un nœud



La configuration de démarrage du nœud de données reste inchangée afin que vous puissiez rajouter le nœud de données ultérieurement sans perdre votre configuration.

Étape 3 Cliquez sur **Apply** (Appliquer).

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement un membre, vous devez rejoindre manuellement la grappe.

Procédure

Étape 1 Si vous avez toujours l'accès à ASDM, vous pouvez réactiver la mise en grappe dans ASDM en connectant ASDM au nœud que vous souhaitez réactiver.

Vous ne pouvez pas réactiver la mise en grappe pour un nœud de données à partir du nœud de contrôle, sauf si vous l'ajoutez en tant que nouveau membre.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**.
b) Cochez la case **Participate in ASA cluster** (Participer à la grappe ASA).
c) Cliquez sur **Apply** (Appliquer).

Étape 2 Si vous ne pouvez pas utiliser ASDM : Sur la console, passez en mode de configuration de grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 3 Activez la mise en grappe.

enable

Quitter la grappe

Si vous souhaitez quitter complètement la grappe, vous devez supprimer toute la configuration de démarrage de la grappe. Étant donné que la configuration actuelle sur chaque nœud est la même (synchronisée à partir de l'unité active), quitter la grappe implique également de restaurer une configuration antérieure à la grappe à partir d'une sauvegarde ou d'effacer votre configuration et de recommencer pour éviter les conflits d'adresses IP.

Procédure

Étape 1 Pour un nœud de données, désactivez la mise en grappe :

cluster group *cluster_name* **no enable**

Exemple :

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

Vous ne pouvez pas modifier la configuration lorsque la mise en grappe est activée sur un nœud de données.

Étape 2 Effacez la configuration de la grappe :

clear configure cluster

L'ASA désactive toutes les interfaces, y compris l'interface de gestion et la liaison de commande de grappe.

Étape 3 Désactivez le mode d'interface de la grappe :

no cluster interface-mode

Le mode n'est pas stocké dans la configuration et doit être réinitialisé manuellement.

Étape 4 Si vous avez une configuration de sauvegarde, copiez-la dans la configuration en cours d'exécution :

copy *backup_cfg* **running-config**

Exemple :

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

Étape 5 Enregistrez la configuration pour le démarrage :

write memory

Étape 6 Si vous n'avez pas de configuration de sauvegarde, reconfigurez l'accès de gestion. Par exemple, assurez-vous de modifier les adresses IP de l'interface et de restaurer le bon nom d'hôte.

Modifier le nœud de contrôle



Mise en garde La méthode recommandée pour changer le nœud de contrôle est de désactiver la mise en grappe sur celui-ci en attendant un nouveau choix de contrôle, puis de réactiver la mise en grappe. Si vous devez spécifier le nœud exact que vous souhaitez voir devenir le nœud de contrôle, utilisez la procédure décrite dans cette section. Notez toutefois que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle à l'aide de cette procédure, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Pour modifier le nœud de contrôle, procédez comme suit.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Summary (Résumé de la grappe)**.

Étape 2 Dans la liste déroulante, choisissez un nœud de données pour devenir le contrôle et cliquez sur le bouton pour en faire le nœud de contrôle.

Étape 3 Vous êtes invité à confirmer le changement de nœud de contrôle. Cliquez sur **Oui**.

Étape 4 Quittez ASDM et reconnectez-vous en utilisant l'adresse IP de la grappe principale.

Exécuter une commande à l'échelle de la grappe

Pour envoyer une commande à tous les nœuds de la grappe ou à un nœud en particulier, procédez comme suit. L'envoi d'une commande **show** à tous les nœuds collecte toutes les sorties et les affiche sur la console

du nœud actuel. D'autres commandes, telles que **capture** et **copy**, peuvent également profiter d'une exécution à l'échelle de la grappe.

Avant de commencer

Effectuez cette procédure au niveau de l'outil d'interface de ligne de commande : choisissez **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**.

Procédure

Envoyez une commande à tous les nœuds ou, si vous spécifiez le nom du nœud, à un nœud en particulier :

cluster exec [**unit** *node_name*] *command*

Exemple :

```
ciscoasa# cluster exec show xlate
```

Pour afficher les noms de nœud, saisissez **cluster exec unit ?** (unité d'exécution de grappe?) (pour voir tous les noms à l'exception du nœud actuel), ou saisissez la commande **show cluster info**.

Exemples

Pour copier simultanément le même fichier de capture de tous les nœuds de la grappe vers un serveur TFTP, saisissez la commande suivante sur le nœud de contrôle :

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Plusieurs fichiers PCAP, un pour chaque nœud, sont copiés sur le serveur TFTP. Le nom du fichier de capture de destination est automatiquement associé au nom du nœud, par exemple capture1_asa1.pcap, capture1_asa2.pcap, etc. Dans cet exemple, asa1 et asa2 sont des noms de nœuds de grappe.

Supervision de la grappe ASA virtuel

Vous pouvez superviser et dépanner l'état de la grappe et les connexions.

Supervision de l'état de la grappe

Consultez les écrans suivantes pour superviser l'état de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Cluster Summary (Résumé de la grappe)**

  Ce volet affiche des renseignements sur la grappe concernant le nœud auquel vous êtes connecté, ainsi que les autres nœuds de la grappe. Vous pouvez également modifier le nœud principal à partir de ce volet.

- **Tableau de bord de la grappe**

  Sur la page d'accueil du nœud principal, vous pouvez superviser la grappe à l'aide des tableaux de bord de grappe et de pare-feu de grappe.

Capture des paquets à l'échelle de la grappe

Consultez l'écran suivante pour capturer des paquets dans une grappe :

Wizards (Assistants) > Packet Capture Wizard (Assistant de capture de paquets)

Pour prendre en charge le dépannage à l'échelle de la grappe, vous pouvez activer la capture du trafic spécifique à la grappe sur le nœud de contrôle, qui est ensuite automatiquement activée sur tous les nœuds de données de la grappe.

Supervision des ressources de la grappe

Consultez les écrans suivants pour surveiller les ressources de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > System Resources Graphs (Graphiques de ressources système) > CPU (Processeur)**

  Ce volet vous permet de créer des graphiques ou des tableaux montrant l'utilisation du processeur sur les nœuds de la grappe.

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > System Resources Graphs (Graphiques de ressources système) > Memory (Mémoire)**. Ce volet vous permet de créer des graphiques ou des tableaux montrant la mémoire libre et la mémoire utilisée sur les nœuds de la grappe.

Supervision du trafic de la grappe

Consultez les commandes suivants pour superviser le trafic de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Trafic Graphs (Graphiques du trafic) > Connections (Connexions)**.

  Ce volet vous permet de créer des graphiques ou des tableaux montrant les connexions entre les membres de la grappe.

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Trafic Graphs (Graphiques du trafic) > Throughput (Débit)**.

  Ce volet vous permet de créer des graphiques ou des tableaux montrant le débit du trafic entre les membres de la grappe.

- **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Load-Monitoring (Supervision de la charge de la grappe)**

  Cette section comprend les volets **Load Monitor-Information** (Renseignements sur le moniteur de charge) et **Load-Monitor Details** (Détails du moniteur de charge). **Load Monitor-Information** (Renseignements sur le moniteur de charge) affiche la charge de trafic pour les membres de la grappe pour le dernier intervalle ainsi que la moyenne du nombre total d'intervalles configurés (30 par défaut). Utilisez le volet **Load-Monitor Details** (Détails du moniteur de charge) pour afficher la valeur de chaque mesure à chaque intervalle.

Supervision de la liaison de commande de grappe

Consultez l'écran suivant pour superviser l'état de la grappe :

Monitoring (Supervision) > Properties (Propriétés) > System Resources Graphs (Graphiques des ressources du système) > Cluster Control Link (Liaison de commande de grappe).

Ce volet vous permet de créer des graphiques ou des tableaux indiquant l'utilisation de la capacité de réception et de transmission de la liaison de commande de grappe.

Supervision du routage de la grappe

Consultez l'écran suivant pour le routage de la grappe :

- **Monitoring (Supervision)** > **Routing (Routage)** > **LISP-EID Table (Tableau LISP-EID)**

  Affiche le tableau EID de l'ASA qui indique les EID et les ID de site.

Configuration de la journalisation pour la mise en grappe

Consultez l'écran suivante pour configurer la journalisation pour la mise en grappe :

Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Setup (Configuration du journal système)

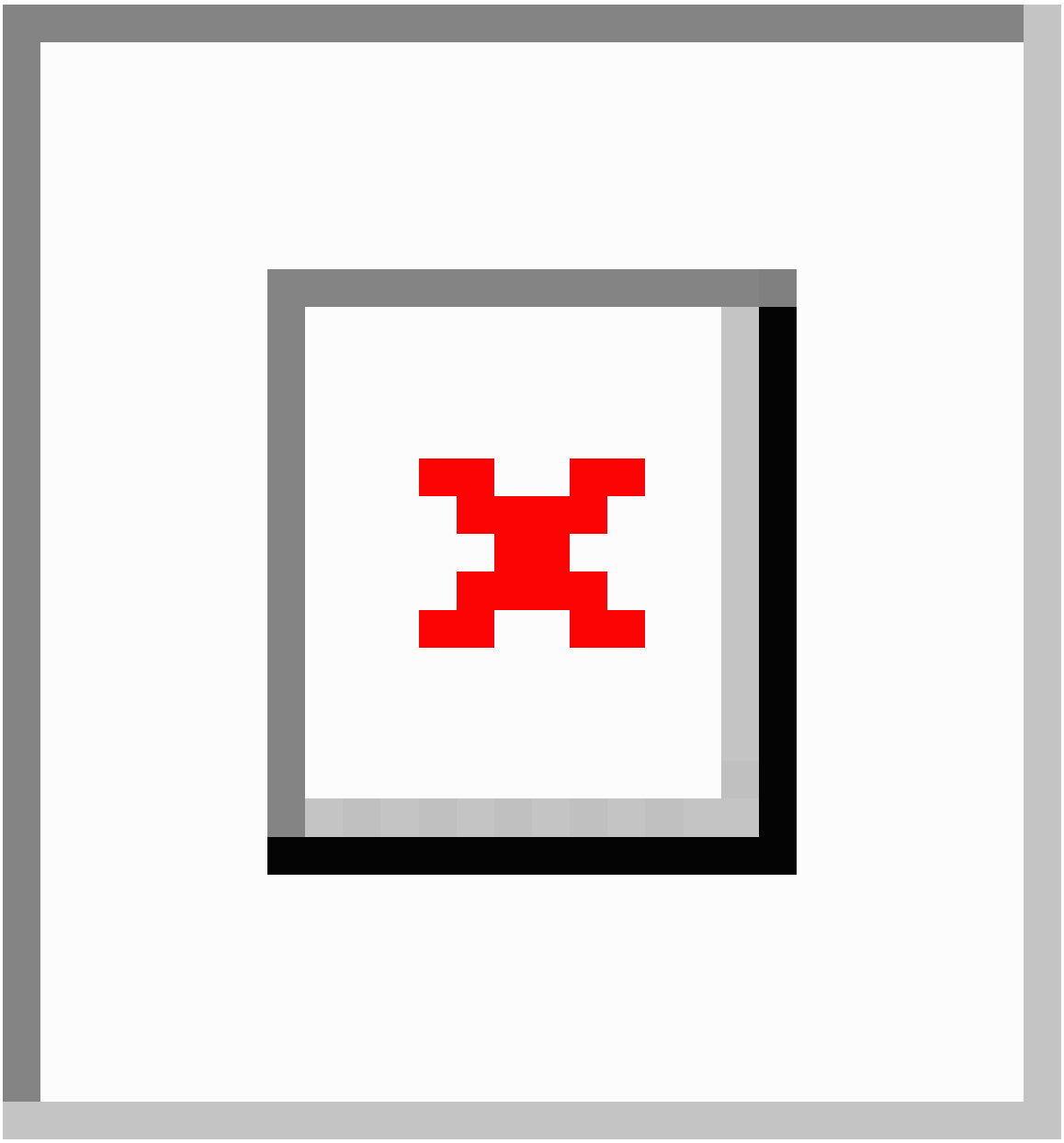
Chaque nœud de la grappe génère des messages de journal système de manière indépendante. Vous pouvez pour générer des messages de journal système avec des ID de périphérique identiques ou différents afin de faire apparaître les messages comme provenant de nœuds identiques ou différents dans la grappe.

Exemples de mise en grappe d'ASA virtuel

Ces exemples incluent toutes les configurations ASA liées aux grappes pour les déploiements typiques.

Exemple inter-sites nord-sud de mode routé d'interface individuelle

L'exemple suivant montre 2 nœuds de grappe ASA dans chacun des 2 centres de données placés entre les routeurs internes et externes (insertion nord-sud). Les nœuds de la grappe sont connectés par la liaison de commande de grappe sur l'interface DCI. Les routeurs internes et externes de chaque centre de données utilisent OSPF et PBR ou ECMP pour équilibrer la charge du trafic entre les membres de la grappe. En attribuant un routage à coût plus élevé sur l'interface DCI, le trafic reste dans chaque centre de données, sauf si tous les nœuds de la grappe ASA d'un site donné tombent en panne. En cas de défaillance de tous les nœuds de la grappe sur un site, le trafic passe de chaque routeur sur l'interface DCI aux nœuds de la grappe ASA sur l'autre site.



Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités et mise en grappe de l'ASA

Certaines fonctionnalités d'ASA ne sont pas prises en charge avec la mise en grappe d'ASA, et d'autres le sont uniquement sur le nœud de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités non prises en charge par la mise en grappe

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

- Fonctionnalités de communication unifiée qui reposent sur le mandataire TLS
- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Interfaces de tunnel virtuel (VTI)
- Les inspections d'application suivantes :
  - CTIQBE
  - H323, H225 et RAS
  - Intercommunication IPsec
  - MGCP
  - MMP
  - RTSP
  - SCCP (Skinny)
  - WAAS
  - WCCP
- Filtre de trafic de réseau de zombies
- Auto Update Server
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Équilibrage de la charge VPN
- Basculement
- Routage et pont intégrés
- Mode FIPS

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.

Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

- Ces inspections d'application sont prises en charge :
  - DCERPC et ESMTP
  - IM
  - NetBIOS et PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET et SUNRPC
  - TFTP
  - XDMCP
- Surveillance du routage statique
- Autorisation et authentification pour l'accès réseau La comptabilité est décentralisée.
- Services de filtrage
- VPN de site à site
- Routage multidiffusion

Fonctionnalités appliquées aux nœuds individuels

Ces fonctionnalités sont appliquées à chaque nœud ASA, plutôt qu'à la grappe dans son ensemble ou au nœud de contrôle.

- QoS : la politique QoS est synchronisée dans la grappe dans le cadre de la duplication de la configuration. Cependant, la politique est appliquée sur chaque nœud indépendamment. Par exemple, si vous configurez le contrôle en sortie, les valeurs de débit de conformité et de rafale de conformité s'appliquent au trafic sortant d'un ASA particulier. Dans une grappe à 3 nœuds et avec le trafic réparti uniformément, le taux de conformité devient en fait trois fois supérieur au débit de la grappe.
- Détection des menaces : la détection des menaces fonctionne sur chaque nœud indépendamment; par exemple, les statistiques principales sont propres au nœud. La détection de l'analyse de port, par exemple, ne fonctionne pas, car l'analyse du trafic sera équilibrée entre tous les nœuds et un nœud ne verra pas tout le trafic.

- Gestion des ressources : la gestion des ressources en mode contexte multiple est appliquée séparément sur chaque nœud en fonction de l'utilisation locale.
- Trafic LISP : le trafic LISP sur le port UDP 4342 est inspecté par chaque nœud de réception, mais aucun directeur n'est affecté. Chaque nœud ajoute au tableau EID qui est partagé dans la grappe, mais le trafic LISP lui-même ne participe pas au partage de l'état de la grappe.

AAA pour l'accès réseau et la mise en grappe

L'AAA pour l'accès réseau comprend trois composants : l'authentification, l'autorisation et la gestion de comptes. L'authentification et l'autorisation sont mises en œuvre en tant que fonctionnalités centralisées sur le nœud de contrôle de mise en grappe avec la duplication des structures de données sur les nœuds de données de grappe. Si un nœud de contrôle est choisi, le nouveau nœud de contrôle disposera de toute l'information nécessaire pour continuer le fonctionnement ininterrompu des utilisateurs authentifiés établis et de leurs autorisations associées. Les délais d'inactivité et absolus pour l'authentification des utilisateurs sont conservés lorsqu'un changement de nœud de contrôle se produit.

La comptabilité est mise en œuvre en tant que fonctionnalité distribuée dans une grappe. La comptabilité est effectuée flux par flux, de sorte que le nœud de la grappe possédant un flux enverra les messages de démarrage et d'arrêt de comptabilité au serveur AAA lorsque la comptabilité est configurée pour un flux.

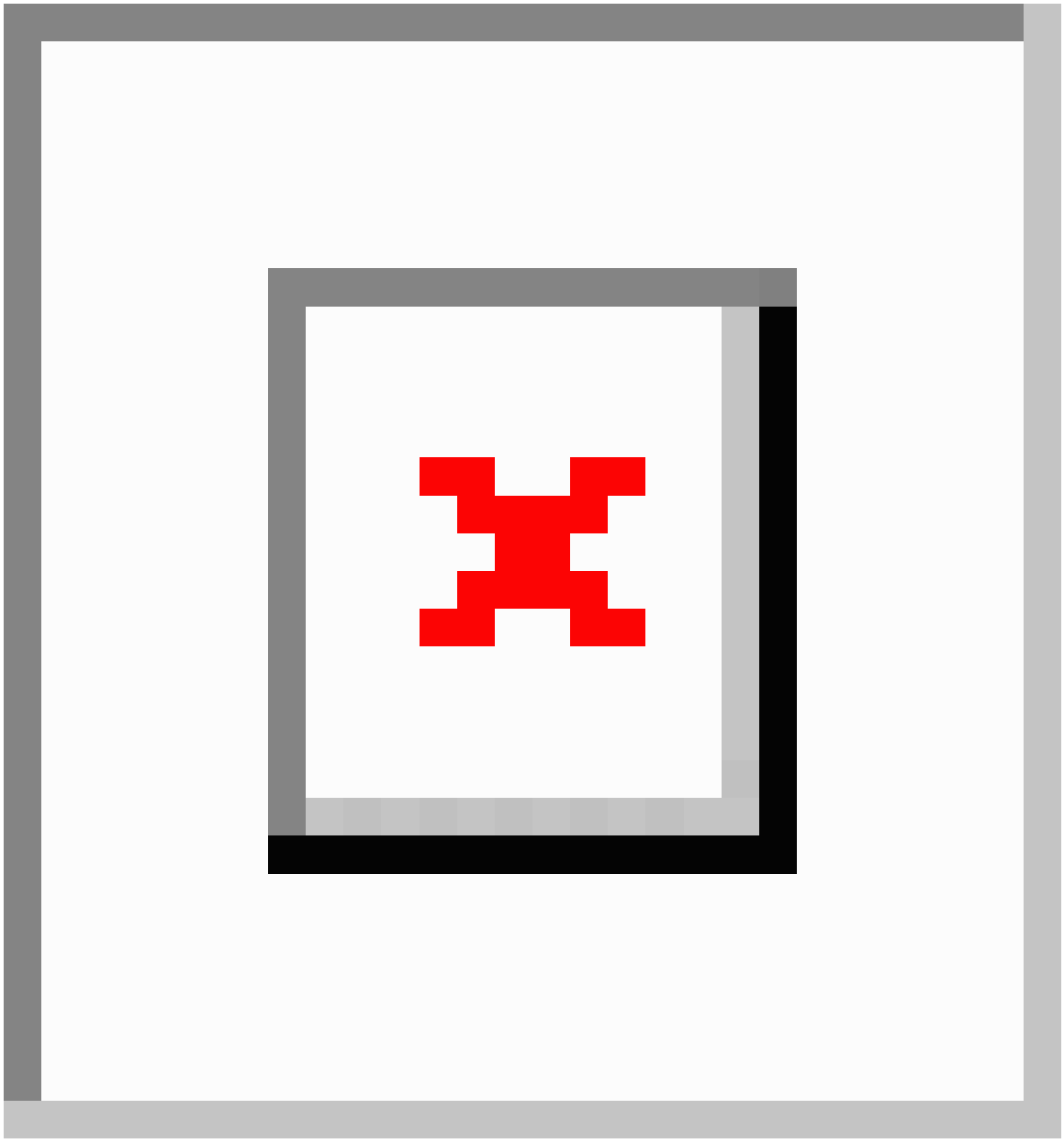
Paramètres de connexion et mise en grappe

Les limites de connexion s'appliquent à l'ensemble de la grappe (voir **Configuration** > **Firewall** > **Service Policy**, page). Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

Routage et mise en grappe dynamiques

En mode d'interface individuel, chaque nœud exécute le protocole de routage en tant que routeur autonome, et les routes sont apprises par chaque nœud indépendamment.

Illustration 68 : Routage dynamique en mode d'interface individuelle



Dans le diagramme ci-dessus, le routeur A détecte qu'il existe quatre chemins à coûts égaux vers le routeur B, chacun passant par un nœud. ECMP est utilisé pour équilibrer la charge du trafic entre les quatre chemins. Chaque nœud choisit un ID de routeur différent lorsqu'il communique avec des routeurs externes.

Vous devez configurer un groupement de grappes pour l'ID de routeur afin que chaque nœud ait un ID de routeur distinct.

Le protocole EIGRP ne forme pas de relations de voisinage avec les homologues de la grappe en mode d'interface individuelle.

Remarque Si la grappe comporte plusieurs contiguïtés avec le même routeur à des fins de redondance, le routage dissymétrique peut entraîner une perte de trafic inacceptable. Pour éviter le routage dissymétrique, regroupez toutes ces interfaces de nœud dans la même zone de trafic. Voir Configurer une zone de trafic, à la page 750.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.
- Si vous utilisez l'AAA pour l'accès FTP, le flux du canal de contrôle est centralisé sur le nœud de contrôle.

Inspection ICMP et mise en grappe

Le flux des paquets d'erreurs ICMP et ICMP dans la grappe varie selon que l'inspection d'erreurs ICMP ou ICMP est activée ou non. Sans inspection ICMP, ICMP est un flux unidirectionnel et il n'y a pas de prise en charge de flux directeur. Avec l'inspection ICMP, le flux ICMP devient bidirectionnel et est soutenu par un flux directeur/de sauvegarde. L'une des différences avec un flux ICMP inspecté réside dans le traitement par le directeur du paquet transféré : le directeur transmettra le paquet de réponse d'écho ICMP au propriétaire du flux au lieu de retourner le paquet au transitaire.

Routage multidiffusion et mise en grappe

En mode d'interface individuel, les unités n'agissent pas indépendamment avec la multidiffusion. Toutes les données et les paquets de routage sont traités et transmis par l'unité de contrôle, évitant ainsi la duplication des paquets.

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents ASAdans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à ASA qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

- No Proxy ARP (Pas de serveur mandataire ARP) : pour les interfaces individuelles, une réponse de serveur mandataire ARP n'est jamais envoyée pour les adresses mappées. Cela empêche le routeur adjacent de maintenir une relation d'homologue avec un ASA qui ne fait plus partie de la grappe. Le routeur en amont a besoin d'une route statique ou d'un PBR avec suivi d'objets pour les adresses mappées qui pointe vers l'adresse IP de la grappe principale. Ce n'est pas un problème pour un EtherChannel étendu, car il n'y a qu'une seule adresse IP associée à l'interface de grappe.

- No interface PAT on an Individual interface (Pas de PAT d'interface sur une interface individuelle) Le PAT d'interface n'est pas pris en charge pour les interfaces individuelles.

- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :
  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.
  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraîneront des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouvel ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.
  - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.

- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, la grappe divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.

- Réutiliser un pool PAT dans plusieurs règles : pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interfaces dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.

- Pas de tourniquet : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.

- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.

- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.

- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité

supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.

- Fonctionnalité PAT par session : bien qu'elle ne soit pas exclusive à la mise en grappe, la fonctionnalité PAT par session améliore l'évolutivité de PAT et, pour la mise en grappe, permet à chaque nœud de données de posséder des connexions PAT; en revanche, les connexions PAT multisessions doivent être transférées au nœud de contrôle et détenues par celui-ci. Par défaut, tout le trafic TCP et le trafic DNS UDP utilisent un xlate PAT par session, tandis que ICMP et tout le reste du trafic UDP utilise la multisession. Vous pouvez configurer des règles NAT par session pour modifier ces valeurs par défaut pour TCP et UDP, mais vous ne pouvez pas configurer la PAT par session pour ICMP. Par exemple, en raison de l'utilisation croissante du protocole Quic sur le port UDP/443 comme alternative de performance à HTTPS TLS sur TCP/443, vous devriez activer la traduction d'adresses par session (PAT) pour UDP/443. Pour le trafic qui bénéficie de la PAT multisession, comme le H.323, le SIP ou l'interface simplifiée, vous pouvez désactiver la PAT par session pour les ports TCP associés (les ports UDP de ces ports H.323 et SIP sont déjà multisession en par défaut). Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.
- Pas de PAT statique pour les inspections suivantes :
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

SCTP et mise en grappe

Une association SCTP peut être créée sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses connexions multi-hébergement doivent résider sur le même nœud.

Inspection SIP et mise en grappe

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

La configuration du mandataire TLS n'est pas prise en charge.

SNMP et mise en grappe

Un agent SNMP interroge chaque ASA en fonction de l'adresse IP locale de son . Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud.Vous devez les rajouter sur le nœud de contrôle pour forcer les utilisateurs à se reproduire vers le nouveau nœud, ou directement sur le nœud de données.

STUN et mise en grappe

L'inspection STUN est prise en charge dans les modes de basculement et de grappe, car les sténopés sont dupliqués. Cependant, l'ID de transaction n'est pas répliqué sur les nœuds. Dans le cas où un nœud tombe en panne après avoir reçu une demande STUN et qu'un autre nœud a reçu la réponse STUN, la réponse STUN sera abandonnée.

Syslog, NetFlow et la mise en grappe

- Syslog : chaque nœud de la grappe génère ses propres messages de journal système. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.
- NetFlow : chaque nœud de la grappe génère son propre flux NetFlow. Le collecteur NetFlow peut traiter chaque appareil ASA uniquement comme un exportateur NetFlow distinct.

Cisco TrustSec et la mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

VPN et mise en grappe

Le VPN de site à site est une fonctionnalité centralisée; seul le nœud de contrôle prend en charge les connexions VPN.

Remarque L'accès VPN à distance n'est pas pris en charge avec la mise en grappe.

La fonctionnalité VPN est limitée au nœud de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si le nœud de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les utilisateurs de VPN verront une perturbation de service. Lorsqu'un nouveau nœud de contrôle est choisi, vous devez rétablir les connexions VPN.

Pour les connexions à une interface individuelle lors de l'utilisation de PBR ou d'ECMP, vous devez toujours vous connecter à l'adresse IP de la grappe principale, et non à une adresse locale.

Les clés et les certificats liés au VPN sont répliqués sur tous les nœuds.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Calcul du débit

Par exemple, si votre modèle peut gérer environ 10 Gbit/s de trafic lorsqu'il est exécuté seul, pour une grappe de 8 unités, le débit combiné maximal sera d'environ 80 % de 80 Gbit/s (8 unités x 10 Gbit/s) : 64 Gbit/s.

Choix du nœud de contrôle

Les composants clés concernés dans le processus d'élection du nœud de contrôle sont les suivants :

- Nœuds de grappe : communiquent par la liaison de commande de grappe et participent au processus d'élection
- Demandes d'élection : diffusées toutes les 3 secondes par les nœuds lorsque la mise en grappe est activée
- Valeurs de priorité : définies entre 1 et 100, où 1 correspond à la priorité la plus élevée
- Nœud de contrôle : le nœud choisi qui coordonne les opérations de la grappe

Ces étapes décrivent comment les nœuds de la grappe élisent un nœud de contrôle :

1. Lorsque la mise en grappe est activée pour un nœud (ou lorsque celui-ci démarre pour la première fois alors que la mise en grappe est déjà activée), le nœud diffuse une demande d'élection toutes les 3 secondes.
2. Tout autre nœud ayant une priorité plus élevée répond à la demande d'élection. La priorité est comprise entre 1 et 100, 1 représentant la priorité la plus élevée.
3. Si, après 45 secondes, un nœud ne reçoit pas de réponse d'un autre nœud de priorité plus élevée, il devient le nœud de contrôle.



Remarque Si plusieurs nœuds sont à égalité pour la priorité la plus élevée, le nom du nœud de la grappe, suivi du numéro de série, est utilisé pour déterminer le nœud de contrôle.

4. Si un nœud rejoint ultérieurement la grappe avec une priorité plus élevée, il ne devient pas automatiquement le nœud de contrôle. Le nœud de contrôle existant conserve toujours son rôle, sauf s'il cesse de répondre, auquel cas un nouveau nœud de contrôle est élu.
5. Dans un scénario de « split brain », où plusieurs nœuds de contrôle sont temporairement présents, le nœud ayant la priorité la plus élevée conserve son rôle tandis que les autres nœuds reprennent leur rôle de nœud de données.

Remarque Vous pouvez forcer manuellement un nœud à devenir le nœud de contrôle. Pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Haute disponibilité au sein de la grappe ASA virtuel

La mise en grappe ASA virtuel assure une disponibilité élevée en surveillant l'intégrité des nœuds et de l'interface et en reproduisant les états de la connexion entre les nœuds.

Supervision de l'intégrité du nœud

Chaque nœud envoie périodiquement un paquet de diffusion heartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet heartbeat ou autre paquet d'un nœud de données au cours du délai d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est élu parmi les nœuds restants.

Scénario de déconnexion cérébrale

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles désignées utilisées et signale les modifications d'état au nœud de contrôle.

Lorsque vous activez la surveillance de l'intégrité, toutes les interfaces physiques sont supervisées par défaut; vous pouvez éventuellement désactiver la surveillance par interface. Seules les interfaces nommées peuvent être surveillées.

Un nœud est supprimé de la grappe en cas de défaillance de ses interfaces surveillées. Le délai avant la suppression par l'ASA d'un membre de la grappe dépend du fait que le nœud est un membre établi ou qu'il rejoint la grappe. L'ASA ne supervise pas les interfaces pendant les 90 premières secondes où un nœud rejoint la grappe. Les changements d'état de l'interface pendant cette période n'entraîneront pas le retrait de l'ASA de la grappe. Le nœud est supprimé après 500 ms, quel que soit son état.

État après l'échec

Lorsqu'un nœud de la grappe tombe en panne, les connexions hébergées par ce nœud sont transférées en toute transparence vers d'autres nœuds; Les renseignements d'état sur les flux de trafic sont partagés sur la liaison de commande de grappe du nœud de contrôle.

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

ASA tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.

Remarque Lorsque ASA devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe, l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Rejoindre la grappe

Après le retrait d'un nœud de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : l'ASA essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment. Ce comportement est configurable.
- Échec de l'interface de données : l'ASA tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'ASA désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe. Ce comportement est configurable.
- Nœud en échec : si le nœud a été supprimé de la grappe en raison d'un échec de vérification de l'intégrité du nœud, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que le nœud rejoindra la grappe au redémarrage, à condition que la liaison de commande de grappe soit active et que la mise en grappe soit toujours activée. L'ASA tente de rejoindre la grappe toutes les 5 secondes.
- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc. Un nœud tentera de rejoindre la grappe automatiquement aux intervalles suivants : 5 minutes, 10 minutes, puis 20 minutes. Ce comportement est configurable.

Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 24 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
Tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	Comprend les règles AAA (uauth).
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—
VPN distribué (site à site) pour Firepower 4100/9300	Oui	La session de sauvegarde devient la session active, puis une nouvelle session de sauvegarde est créée.

Gestion des connexions par la grappe ASA virtuel

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.
- Propriétaire de la sauvegarde : nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

  Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis.

Si vous activez la localisation du directeur pour la mise en grappe inter-sites, il existe deux rôles de propriétaire de la sauvegarde : le rôle de sauvegarde locale et de sauvegarde globale. Le propriétaire choisit toujours une sauvegarde locale sur le même site que lui (en fonction de l'ID du site). La sauvegarde globale peut se trouver sur n'importe quel site et peut même se trouver sur le même nœud que la sauvegarde locale. Le propriétaire envoie des informations sur l'état de la connexion aux deux sauvegardes.

Si vous activez la redondance de sites et que le propriétaire de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La sauvegarde de châssis et la sauvegarde de site sont indépendantes. Par conséquent, dans certains cas, un flux comportera à la fois une sauvegarde de châssis et une sauvegarde de site.

- Directeur : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

  Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Si vous activez la localisation de directeur pour la mise en grappe inter-sites, il y a deux rôles de directeur : le directeur local et le directeur global. Pour un paquet de nouveau flux, le membre de réception sélectionne le directeur local parmi les membres du site du membre de réception. Le directeur global peut se trouver sur n'importe quel site et peut même être le même membre que le directeur local. En cas de défaillance du propriétaire d'origine et lorsque la localisation s'applique, le directeur local choisit un nouveau propriétaire de connexion sur le site du directeur local.

  Détails du hachage ICMP/ICMPv6 :

  - Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
  - Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
  - Pour les autres paquets, les ports source et de destination sont à 0.

- Transitaire : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Si vous activez la localisation de directeur, le redirecteur interroge le directeur local lorsque la localisation s'applique. Le transitaire interroge le directeur global si le directeur local ne connaît pas le propriétaire, si la connexion appartient à un autre site ou si la localisation est contournée. Une requête de directeur intersite est le comportement attendu dans ces cas. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.

Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

- Propriétaire de fragment : pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

Connexions par traduction d'adresse de port

Lorsqu'une connexion utilise la traduction d'adresses de port (PAT), le type de PAT (par session ou multisession) influence quel membre de la grappe devient propriétaire de la nouvelle connexion :

- PAT par session : le propriétaire est le nœud qui reçoit le paquet initial dans la connexion.

  Par défaut, le trafic TCP et DNS UDP utilise une PAT par session.

- PAT multisession : le propriétaire est toujours le nœud de contrôle. Si une connexion PAT multisession est initialement reçue par un nœud de données, le nœud de données transfère la connexion au nœud de contrôle.

  Par défaut, le trafic UDP (à l'exception du trafic UDP DNS) et ICMP utilise la PAT multisession. Ces connexions appartiennent donc toujours au nœud de contrôle.

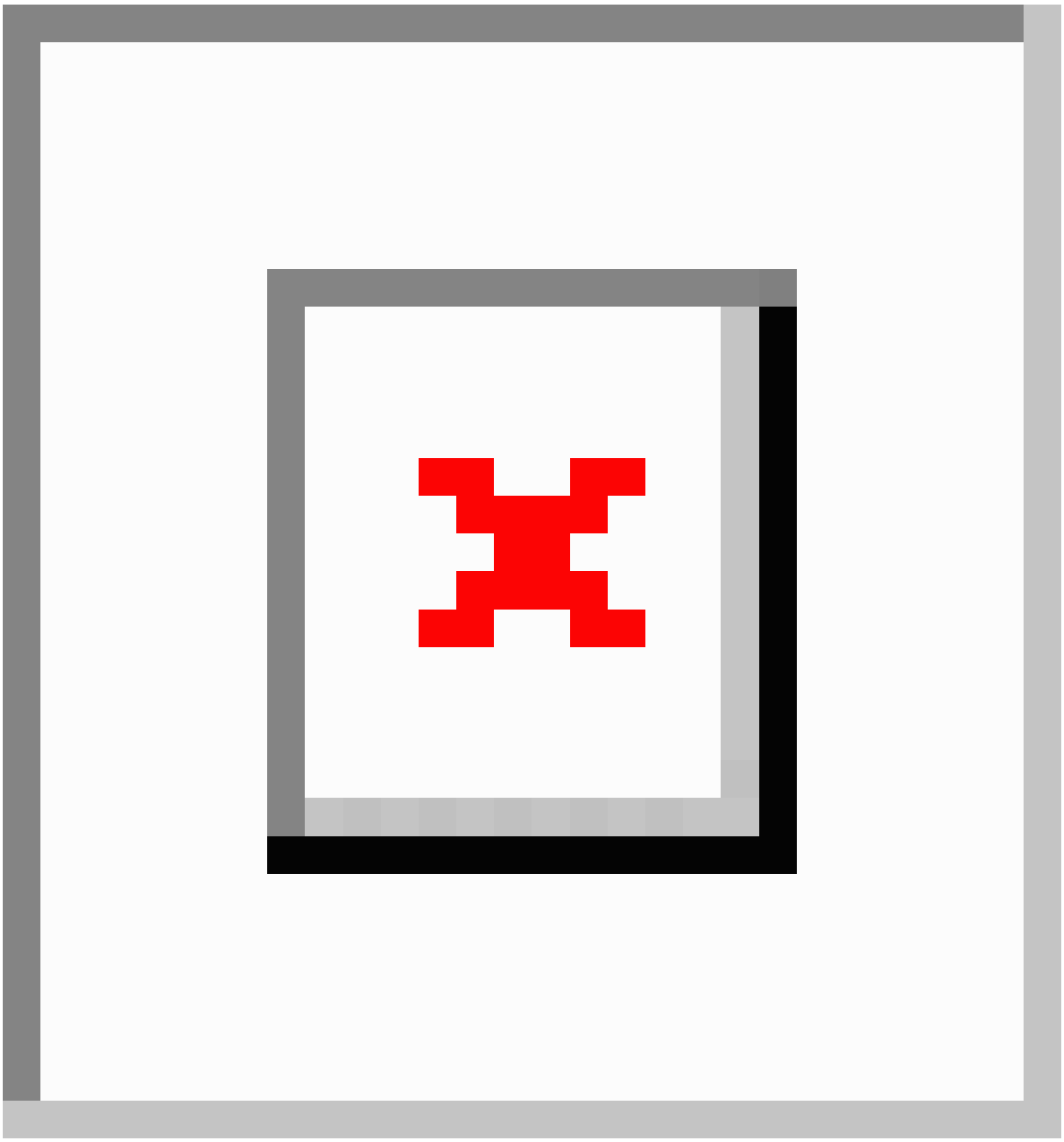
Vous pouvez modifier les valeurs par défaut de PAT par session pour les protocoles TCP et UDP afin que les connexions à ces protocoles soient gérées par session ou multisession selon la configuration. Pour ICMP, vous ne pouvez pas modifier la PAT multisession par défaut. Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Pour de meilleures performances, un bon équilibrage de la charge externe est nécessaire pour que les deux directions d'un flux arrivent au même nœud et pour que les flux soient répartis uniformément entre les nœuds. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.



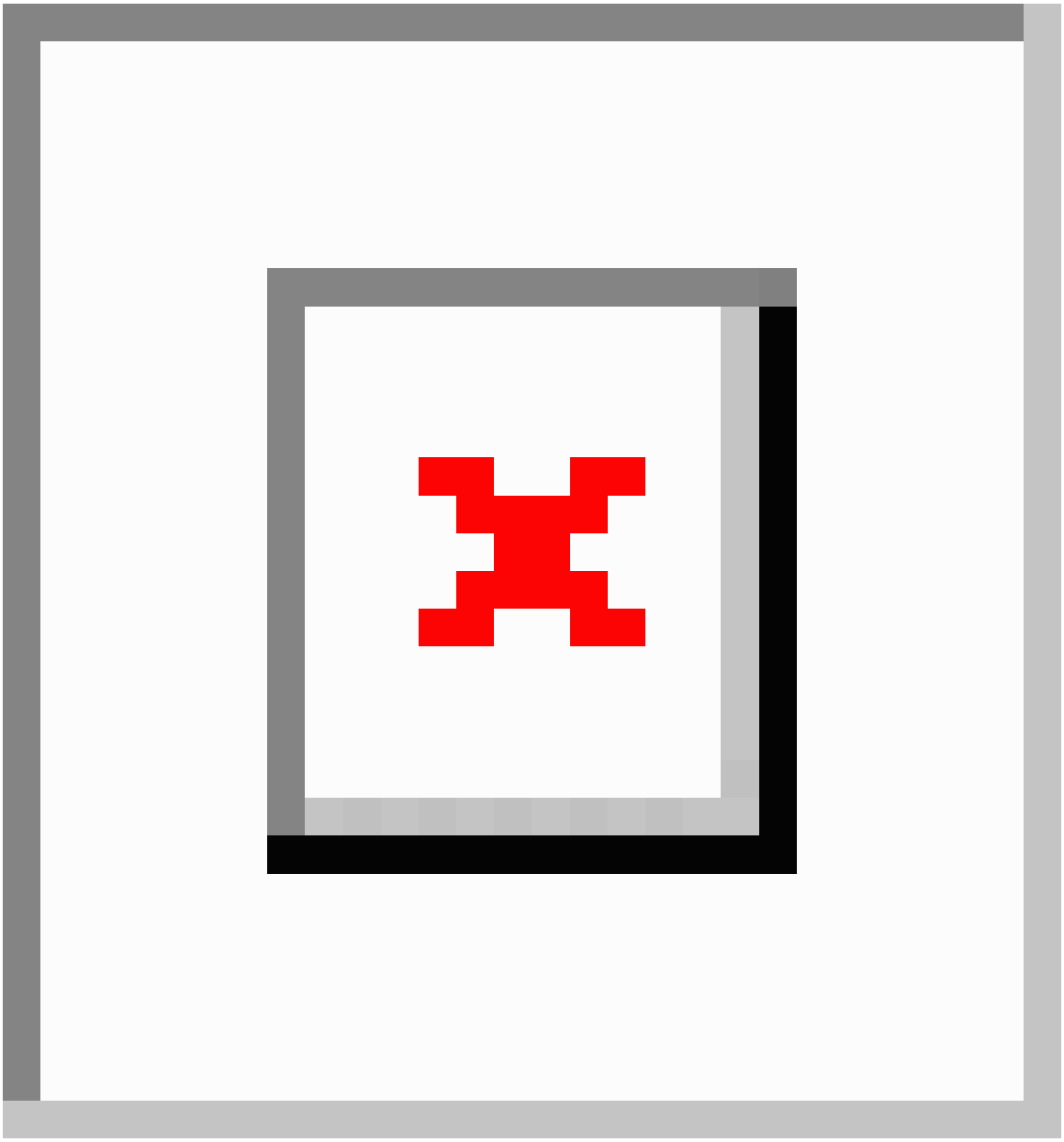
1. Le paquet SYN provient du client et est livré à un ASA (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un ASA différent (selon la méthode d'équilibrage de la charge). Cet ASA est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.

5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.
7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. *Illustration 69 : Flux de données ICMP et UDP*



Le premier paquet UDP provient du client et est remis à un ASA (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.

6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.
8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Rééquilibrage des nouvelles connexions TCP dans la grappe

Si les capacités d'équilibrage de charges des routeurs en amont ou en aval entraînent une répartition non équilibrée des flux, vous pouvez configurer un rééquilibrage des nouvelles connexions afin que les nœuds ayant le plus de nouvelles connexions par seconde redirigent les nouveaux flux TCP vers d'autres nœuds. Aucun flux existant ne sera déplacé vers d'autres nœuds.

Comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal.

Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

Historique de la mise en grappe d'ASA virtuel

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Suppression des propos tendancieux	9.19(1)	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
Mise en grappe d'ASAv30, ASAv50 et ASAv100 pour VMware et KVM	9.17(1)	La mise en grappe d'ASA virtuel vous permet de regrouper jusqu'à 16 ASA virtuel en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques. La mise en grappe d'ASA virtuel prend en charge le mode d'interface individuelle en mode de pare-feu routé; les EtherChannels étendus ne sont pas pris en charge. L'ASA virtuel utilise une interface virtuelle VNI (VXLAN) pour la liaison de commande de grappe. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** • **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**



PARTIE III

Interfaces

- Configuration de l’interface de base, à la page 611
- Configuration de base de l’interface pour les ports de commutation du Firepower 1010, à la page 629
- Interfaces EtherChannel , à la page 639
- Interfaces de boucle avec retour, à la page 653
- Sous-interfaces VLAN, à la page 661
- Interfaces VXLAN, à la page 669
- Interfaces en mode routage et en mode transparent, à la page 693
- Configuration avancée de l’interface, à la page 731
- Zones de circulation, à la page 741



CHAPITRE 15

Configuration de l'interface de base

Ce chapitre comprend la configuration de l'interface de base, y compris les paramètres Ethernet et la configuration de la trame étendue.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà dans l'espace d'exécution système, dans le volet Configuration > Device List (Liste des périphériques), double-cliquez sur **System (système)** sous l'adresse IP du périphérique actif.

Remarque Pour Firepower 2100 en mode plateforme et Châssis Firepower 4100/9300 , vous devez configurer les paramètres de l'interface de base dans le système d'exploitation FXOS. Consultez le guide de configuration ou de démarrage de votre châssis pour en savoir plus.

- À propos de la configuration de l'interface de base, à la page 611
- Lignes directrices pour la configuration de l'interface de base, à la page 614
- Paramètres par défaut pour la configuration de l'interface de base, à la page 614
- Activer l'interface physique et configurer les paramètres Ethernet, à la page 615
- Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000), à la page 618
- Gérer le module réseau pour Cisco Secure Firewall 3100, à la page 619
- Exemples d'interfaces de base, à la page 623
- Historique de la configuration de l'interface de base, à la page 624

À propos de la configuration de l'interface de base

Cette section décrit les fonctionnalités de l'interface et les interfaces spéciales.

Fonctionnalité Auto-MDI/MDIX

Pour les interfaces RJ-45, le paramètre de négociation automatique par défaut inclut également la fonction Auto-MDI/MDIX. La fonction Auto-MDI/MDIX élimine le besoin de câblage croisé en effectuant un croisé interne lorsqu'un câble droit est détecté pendant la phase de négociation automatique. La vitesse ou le duplex doivent être réglés pour qu'ils soient négociés automatiquement afin d'activer Auto-MDI/MDIX pour l'interface.

Si vous définissez explicitement la vitesse et le duplex à une valeur fixe, désactivant ainsi la négociation automatique pour les deux paramètres, Auto-MDI/MDIX est également désactivé. Pour Gigabit Ethernet, lorsque la vitesse et le mode duplex sont définis à 1000 et plein, l'interface négocie toujours automatiquement; par conséquent, Auto-MDI/MDIX est toujours activé et vous ne pouvez pas le désactiver.

Interface de gestion

L'interface de gestion, selon votre modèle, est une interface distincte réservée au trafic de gestion.

Présentation de l'interface de gestion

Vous pouvez gérer l'ASA en vous connectant à :

- Toute interface de trafic entrant
- Une interface *logement*/*port* de gestion dédiée (si disponible pour votre modèle)

Vous devrez peut-être configurer l'accès de gestion à l'interface en fonction de l'Accès de gestion, à la page 1135.

L'interface de *logement*/*port* de gestion

Le tableau suivant présente les interfaces de gestion par modèle.

Tableau 25 : Interfaces de gestion par modèle

Modèle	Management 0/0	Management 0/1	Management 1/0	Management 1/1	Configurable pour le trafic de transit	Sous-interfaces autorisées
Firepower 1000	—	—	—	**Oui**	**Oui**	**Oui**
Firepower de la série 2100	—	—	—	**Oui**	— **Remarque :** techniquement, vous pouvez activer le trafic de transit; toutefois, le débit de cette interface n'est pas suffisant pour les opérations de données.	**Oui**
Secure Firewall 3100	—	—	—	**Oui**	**Oui**	**Oui**

Modèle	Management 0/0	Management 0/1	Management 1/0	Management 1/1	Configurable pour le trafic de transit	Sous-interfaces autorisées
Firepower 4100/9300	S. O. L'ID d'interface dépend de l'interface physique de type gestion que vous avez attribuée au périphérique logique ASA	—	—	—	—	**Oui**
ISA 3000	—	—	—	**Oui**	—	—
ASAv	**Oui**	—	—	—	**Oui**	—

Utiliser n'importe quelle interface pour le trafic de gestion uniquement

Vous pouvez utiliser n'importe quelle interface comme interface de gestion uniquement en la configurant pour le trafic de gestion, y compris une interface EtherChannel.

Interface de gestion pour le mode transparent

En mode de pare-feu transparent, en plus du nombre maximum d'interfaces de trafic autorisé, vous pouvez également utiliser l'interface de gestion (l'interface physique ou une sous-interface (si prise en charge par votre modèle)) en tant qu'interface de gestion distincte uniquement.

Vous ne pouvez pas utiliser d'autres types d'interfaces comme interfaces de gestion.

Pour le Châssis Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion que vous avez attribuée au périphérique logique ASA.

Remarque L'interface de gestion ne fait pas partie d'un groupe de ponts normal. Notez que pour des raisons opérationnelles, elle fait partie d'un groupe de ponts non configurable.

Trafic de gestion uniquement

L'interface de gestion traite uniquement le trafic entrant et sortant et ne peut pas transmettre de trafic de transit. Dans tous les cas, comme les groupes de ponts ne peuvent pas communiquer avec d'autres groupes de ponts, il serait impossible à l'interface de gestion d'acheminer vers un groupe de ponts, ou inversement, même si elle prenait en charge le trafic.

Tableau d'adresses MAC partagées et connexions de commutateurs

En mode de pare-feu transparent, l'interface de gestion met à jour le tableau d'adresses MAC de l'ASA de la même manière qu'une interface de données; par conséquent, vous ne devez pas connecter à la fois une interface de gestion et une interface de données au même commutateur, sauf si vous configurez l'un des ports de commutation en tant que port routé (par défaut, les commutateurs Catalyst partagent une adresse MAC pour

tous les ports de commutation VLAN). Sinon, si le trafic arrive sur l'interface de gestion à partir du commutateur physiquement connecté, l'ASA met à jour le tableau d'adresses MAC pour utiliser l'interface de *gestion* pour accéder au commutateur, au lieu de l'interface de données. Cette action entraîne une interruption temporaire du trafic; pour des raisons de sécurité, l'ASA ne mettra pas à jour le tableau d'adresses MAC pour les paquets du commutateur vers l'interface de données pendant au moins 30 secondes.

Mode contexte multiple

En mode de contexte multiple, vous ne pouvez partager aucune interface, y compris l'interface de gestion, entre les contextes. Pour assurer la gestion par contexte sur les modèles pris en charge, vous pouvez créer des sous-interfaces de l'interface de gestion et attribuer une sous-interface de gestion à chaque contexte. Certains modèles n'autorisent pas les sous-interfaces sur l'interface de gestion. Par conséquent, la gestion par contexte pour ces modèles nécessite que vous vous connectiez à une interface de données. Pour le Châssis Firepower 4100/9300 , l'interface de gestion et ses sous-interfaces ne sont pas reconnues comme des interfaces de gestion spécialement autorisées dans les contextes; vous devez traiter une sous-interface de gestion comme une interface de données dans ce cas et l'ajouter à une BVI.

Lignes directrices pour la configuration de l'interface de base

Mode de pare-feu transparent

Pour le contexte multiple, en mode transparent, chaque contexte doit utiliser des interfaces différentes; vous ne pouvez pas partager une interface entre contextes.

Basculement

Vous ne pouvez pas partager une interface de basculement ou d'état avec une interface de données.

Directives supplémentaires

- Certains services liés à la gestion ne sont pas disponibles jusqu'à ce qu'une interface de non-gestion soit activée et que l'ASA atteigne l'état « Système prêt ». L'ASA génère le message de journal système suivant lorsqu'il est à l'état « Système prêt » :

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

Paramètres par défaut pour la configuration de l'interface de base

Cette section répertorie les paramètres par défaut des interfaces si vous n'avez pas de configuration d'usine par défaut.

État par défaut des interfaces

L'état par défaut d'une interface dépend du type d'interface et du mode de contexte.

En mode de contexte multiple, toutes les interfaces allouées sont activées par défaut, quel que soit l'état de l'interface dans l'espace d'exécution du système. Cependant, pour que le trafic passe par l'interface, celle-ci

doit également être activée dans l'espace d'exécution du système. Si vous désactivez une interface dans l'espace d'exécution du système, cette interface est désactivée dans tous les contextes qui la partagent.

En mode unique ou dans l'espace d'exécution du système, les interfaces ont les états par défaut suivants :

- Interfaces physiques : désactivées.
- Sous-interfaces VLAN : activées. Cependant, pour que le trafic passe par la sous-interface, l'interface physique doit également être activée.
- Interfaces VXLAN VNI : activées.
- Interfaces de canal de port EtherChannel (ISA 3000) : activées. Cependant, pour que le trafic passe par l'EtherChannel, les interfaces physiques des groupes de canaux doivent également être activées.
- Interfaces de canal de port EtherChannel (autres modèles) : désactivées.



Remarque Dans le cas du Firepower 4100/9300, vous pouvez activer et désactiver administrativement les interfaces dans le châssis et sur l'ASA. Pour qu'une interface soit opérationnelle, elle doit être activée dans les deux systèmes d'exploitation. Étant donné que l'état de l'interface est contrôlé indépendamment, il se peut que vous ayez une incompatibilité entre le châssis et l'ASA.

Vitesse par défaut et duplex

- Par défaut, la vitesse et les interfaces duplex pour les interfaces en cuivre (RJ-45) sont à négociation automatique.

Type de connecteur par défaut

Certains modèles comprennent deux types de connecteurs : le RJ-45 en cuivre et le SFP à fibre optique. RJ-45 est le type par défaut. Vous pouvez configurer l'ASA pour utiliser les connecteurs SFP à fibre optique.

Adresses MAC par défaut

Par défaut, l'interface physique utilise l'adresse MAC rémanente, et toutes les sous-interfaces d'une interface physique utilisent la même adresse MAC rémanente.

Activer l'interface physique et configurer les paramètres Ethernet

Cette section décrit comment :

- Activer l'interface physique
- Définir une vitesse et un duplex (si disponible)
- Activer les trames de pause pour le contrôle de flux
- Configuration de la correction d'erreurs sans voie de retour

Cette procédure ne couvre qu'un petit sous-ensemble des paramètres de l'interface. S'abstenir de définir d'autres paramètres à ce stade. Par exemple, vous ne pouvez pas nommer une interface que vous souhaitez utiliser dans une interface EtherChannel. Les options d'interface exactes varient selon votre modèle et votre type d'interface.

Remarque Pour le Firepower 4100/9300, vous configurez les paramètres de base de l'interface dans FXOS.

Remarque Pour les ports de commutation / 1010/ , consultez Configuration de base de l'interface pour les ports de commutation du Firepower 1010, à la page 629.

Avant de commencer

Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, dans le volet **Configuration** > **Device List (Liste des périphériques)**, double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Selon votre mode de contexte :

- Pour le mode unique, choisissez le volet **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces**.
- Pour le mode multiple dans l'espace d'exécution du système, choisissez le volet **Configuration > Context Management (Gestion des contextes) > Interfaces** .

Par défaut, toutes les interfaces physiques sont répertoriées.

Étape 2 Cliquez sur une interface physique que vous souhaitez configurer, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche.

Remarque En mode unique, cette procédure ne couvre qu'un sous-ensemble des paramètres de la boîte de dialogue **Edit Interface** (Modifier l'interface). Notez qu'en mode de contexte multiple, avant de terminer la configuration de l'interface, vous devez attribuer des interfaces aux contextes.

Étape 3 Pour activer l'interface, cochez la case **Enable Interface** (Activer l'interface).

Étape 4 Pour ajouter une description, saisissez du texte dans le champ Description.

La description peut contenir jusqu'à 240 caractères sur une seule ligne (sans retour chariot). Dans le cas d'une liaison de basculement ou d'état, la description fixe est « LAN Failover Interface », « STATE Failover Interface » ou « LAN/STATE Failover Interface » par exemple. Vous ne pouvez pas modifier cette description. La description fixe remplace toute description que vous saisissez ici si vous faites de cette interface une liaison de basculement ou un lien d'état.

Étape 5 Pour activer les trames de pause (XOFF) pour le contrôle de flux, cochez la case **Flow-Control** (Contrôle de flux).

Le contrôle de flux permet aux ports Ethernet connectés de contrôler les débits de trafic en cas de congestion en permettant aux nœuds encombrés de suspendre les opérations de liaison à l'autre extrémité. Si le port ASA est congestionné (épuisement des ressources en file d'attente sur le commutateur interne) et ne peut plus recevoir de trafic, il en informe l'autre port en envoyant une trame de pause pour interrompre l'envoi jusqu'à ce que la condition soit réglée. À la réception d'une trame de pause, le périphérique expéditeur arrête d'envoyer des paquets de données, ce qui empêche toute perte de paquets de données pendant la période de congestion.



Remarque L'ASA prend en charge la transmission de trames de pause afin que l'homologue distant puisse contrôler le débit du trafic.

Cependant, la réception de trames de pause n'est pas prise en charge.

Le commutateur interne dispose d'un ensemble global de 8 000 tampons de 250 octets chacun et le commutateur alloue des tampons de manière dynamique à chaque port. Une trame de pause est envoyée à chaque interface pour laquelle le contrôle de flux est activé lorsque l'utilisation de la mémoire tampon dépasse la borne supérieure globale (2 Mo (8 000 tampons)); et une trame de pause est envoyée par une interface particulière lorsque sa mémoire tampon dépasse le seuil supérieur du port (0,3125 Mo (1 250 tampons)). Après l'envoi d'une pause, une trame XON peut être envoyée lorsque l'utilisation de la mémoire tampon est réduite sous le seuil des faibles niveaux (1,25 Mo dans l'ensemble (5 000 tampons ; 0,25 Mo par port (1 000 tampons)). Le partenaire de liaison peut reprendre le trafic après avoir reçu une trame XON.

Seules les trames de contrôle de flux définies dans la norme 802.3x sont prises en charge. Le contrôle de flux basé sur la priorité n'est pas pris en charge.

Étape 6 (Facultatif) Pour définir le type de support, les conditions de duplex, la vitesse et activer les trames de pause pour le contrôle de flux, cliquez sur **Configure Hardware Properties** (Configurer les propriétés matérielles).

a) Pour définir les conditions de **duplex**, choisissez **Full** (Intégral), **Half** (Semi-duplex) ou **Auto** (Automatique), selon le type d'interface dans la liste déroulante.



Remarque Les interfaces SFP prennent uniquement en charge les conditions de duplex intégral.

b) Pour définir la **vitesse**, choisissez une valeur dans la liste déroulante (varie selon le modèle).

Pour les interfaces SFP Firepower 1000 et 2100, le paramètre **Negotiate** définit la vitesse à 1 000 Mbit/s et active la négociation de liaison pour les paramètres de contrôle de flux et les renseignements sur les défaillances à distance. Pour les interfaces de 10 Gbit/s, cette option définit la vitesse à 1 000 Mbit/s. L'option **Nonegotiate** (Aucune négociation) désactive la négociation de liaison.Pour d'autres options de négociation automatique de modèle, consultez la case **Auto-negotiate** (Négociation automatique) de l'onglet **Advanced** (Avancé), qui vous permet d'activer ou de désactiver la négociation automatique sur toute interface de 1 000 Mbit/s et plus.

Choisissez **Detect SFP** (Détecter SFP) pour détecter la vitesse du module SFP installé et utiliser la vitesse appropriée. Le duplex est toujours réglé sur intégral, la négociation automatique est activée et la FEC est réglée sur Auto Pour les émetteurs-récepteurs à double vitesse, la vitesse inférieure est utilisée. Cette option est utile si vous modifiez ultérieurement le module de réseau pour un modèle différent et que vous souhaitez que la vitesse se mette à niveau automatiquement. Certains commutateurs et émetteurs-récepteurs

ne prennent pas en charge la négociation automatique, en particulier pour les interfaces à vitesse plus élevée. Dans ce cas, réglez l'interface ASA à une vitesse manuelle et désactivez également **Auto-negotiate** (Négociation automatique) afin que la liaison puisse s'établir.

c) Pour définir le **FEC Mode** (Mode de correction d'erreurs sans voie de retour) pour les interfaces de 25 Gbit/s et plus, choisissez une valeur dans la liste déroulante.

Pour une interface membre d'EtherChannel, vous devez configurer la correction d'erreur directe avant de l'ajouter à l'EtherChannel. Si vous supprimez l'interface de l'EtherChannel, après le redémarrage, vous devrez peut-être reconfigurer la FEC pour l'interface.

Certains commutateurs ne prennent pas en charge le mode automatique pour la FEC, en particulier pour les interfaces de plus grande taille. Assurez-vous de désactiver la FEC ou de configurer manuellement le paramètre, en fonction de la prise en charge du commutateur.

Le paramètre choisi lorsque vous utilisez **auto** dépend du type d'émetteur-récepteur et selon si l'interface est fixe (intégrée) ou sur un module de réseau.

Tableau 26 : FEC par défaut pour le réglage automatique

Type d'émetteur/récepteur	FEC par défaut du port fixe	FEC par défaut du module de réseau
25G-SR	cl108-rs	cl108-rs
25G-LR	cl108-rs	cl108-rs
10/25G-CSR	cl108-rs	cl74-fc
25G-AOC*x*M	cl74-fc	cl74-fc
25G-CU2.5/3M	Négociation automatique	Négociation automatique
25G-CU4/5M	Négociation automatique	Négociation automatique

d) Cliquez sur **OK** pour accepter les modifications apportées aux **Hardware Properties** (Propriétés matérielles).

Étape 7 Cliquez sur **OK** pour accepter les modifications apportées à l'**Interface**.

Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000)

Une trame étendue est un paquet Ethernet supérieur au maximum standard de 1518 octets (y compris l'en-tête de couche 2 et l'en-tête VLAN) qui peut s'élever jusqu'à 9216 octets. Vous pouvez activer la prise en charge des trames étendues pour toutes les interfaces en augmentant la quantité de mémoire nécessaire pour traiter les trames Ethernet. L'attribution de plus de mémoire aux trames étendues peut limiter l'utilisation maximale d'autres fonctionnalités, telles que les listes de contrôle d'accès. Remarque : la MTU ASA définit la taille de la charge utile sans inclure la couche 2 (14 octets) et l'en-tête VLAN (4 octets), donc la MTU maximale peut s'élever à 9198, selon votre modèle.

Cette procédure s'applique uniquementà l'ISA 3000, et à l'ASA virtuel. D'autres modèles prennent en charge les bâtis grand format par défaut.

Les bâtis grand format ne sont pas pris en charge sur les ASAv5 et ASAv10 avec moins de 8 Go de RAM.

Avant de commencer

- En mode contexte multiple, définissez cette option dans l'espace d'exécution du système.
- Les modifications de ce paramètre nécessitent que vous rechargiez l'ASA.
- Assurez-vous de définir la MTU pour chaque interface devant transmettre des trames étendues à une valeur supérieure à la valeur par défaut 1500; par exemple, définissez la valeur sur 9198. En mode contexte multiple, définissez la MTU dans chaque contexte.
- Veillez à régler le TCP MSS, soit pour le désactiver pour le trafic non-IPsec, soit pour l'augmenter en fonction de la MTU.

Procédure

Selon votre mode de contexte :

- Mode multiple : Pour activer la prise en charge des trames étendues, sélectionnez **Configuration > Context Management (gestion de contexte) > Interfaces**, puis cliquez **Enable jumbo frame support**.
- Mode simple : Le réglage de la MTU à plus de 1500 octets active automatiquement les trames étendues. Pour activer ou désactiver manuellement ce paramètre, sélectionnez **Configuration > Device Setup (configuration du périphérique) > Interface Settings (paramètres de l'interface) > Interfaces**, puis cliquez dans la case à cocher **Enable jumbo frame support**.

Gérer le module réseau pour Cisco Secure Firewall 3100

Si vous installez un module de réseau avant de mettre le pare-feu sous tension pour la première fois, aucune action n'est requise; le module de réseau est activé et prêt à l'emploi.

Si vous devez apporter des modifications à l'installation de votre module de réseau après le démarrage initial, consultez les procédures suivantes.

Configurer les ports d'éclatement

Vous pouvez configurer des ports d'éclatement plus petits pour chaque interface de 40 Gbit/s ou plus. Cette procédure vous indique comment diviser et regrouper les ports. Les ports d'éclatement peuvent être utilisés comme n'importe quel autre port Ethernet physique, y compris lorsqu'ils sont ajoutés aux EtherChannels. Par exemple, vous pouvez répartir quatre ports de 10 Gbit/s à partir d'une interface de 40 Gbit/s. La taille exacte et le nombre de ports dépendent de votre modèle.

Si une interface est déjà utilisée dans votre configuration, vous devrez supprimer manuellement toute configuration liée aux interfaces qui ne seront plus présentes.

Avant de commencer

- Vous devez utiliser un câble épanoui pris en charge. Consultez le guide d'installation du matériel pour plus d'informations.
- Pour la mise en grappe ou le basculement, assurez-vous que la liaison de basculement n'utilise pas l'interface parent (pour la séparation) ou l'interface enfant (pour la jonction); vous ne pouvez pas apporter de modifications à l'interface si elle est utilisée pour la liaison de grappe/basculement.

Procédure

Étape 1 Séparez les ports à partir d'une ou plusieurs interfaces de 40 Go ou plus en sélectionnant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM**, et en saisissant un ou plusieurs **Port Numbers** (Numéros de port) que vous souhaitez diviser, séparés par des virgules (sans espace).

Le logement est toujours **2**.

Par exemple, pour séparer les interfaces Ethernet2/1 et Ethernet 2/2, vous devez spécifier **1,2** dans le champ **Port Number** (Numéro de port). Les interfaces enfants résultantes seront identifiées comme Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3, Ethernet2/1/4, Ethernet2/2/1, Ethernet2/2/2, Ethernet2/2/3 et Ethernet2/2/4.

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; les modifications d'interface sont répliquées sur les autres nœuds.

Étape 2 Joignez les ports d'éclatement pour restaurer l'interface en sélectionnant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM**, et en supprimant un ou plusieurs **Port Numbers** (Numéros de port).

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds.

Vous devez joindre tous les ports enfants d'une interface donnée.

Étape 3 Cliquez sur **Apply** (Appliquer).

La configuration est appliquée au pare-feu.

Ajouter un module de réseau

Pour ajouter un module de réseau à un pare-feu après le démarrage initial, procédez comme suit. L'ajout d'un nouveau module nécessite un rechargement. Pour la mise en grappe ou le basculement, aucun temps d'arrêt n'est pris en charge. Veuillez donc vous assurer d'effectuer cette procédure pendant une fenêtre de maintenance.

Procédure

Étape 1 Installez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez installer le module de réseau lorsque le pare-feu est sous tension.

Pour la mise en grappe ou le basculement, installez le module de réseau sur tous les nœuds.

Étape 2 Rechargez le pare-feu; consultez **Tools (Outils) > System Reload (Rechargement du système)**.

Pour la mise en grappe ou le basculement, rechargez tous les nœuds. Étant donné que les nœuds dotés de modules de réseau différents ne peuvent pas rejoindre la paire de grappe/basculement, vous devez recharger tous les nœuds avec le nouveau module avant qu'ils puissent reformer la paire de grappe/basculement.

Étape 3 Activez le module de réseau en choisissant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM** et en décochant **Disable Netmod** (Désactiver Netmod).

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds.

Étape 4 Cliquez sur **Apply** (Appliquer).

La configuration est appliquée au pare-feu.

Échange à chaud du module de réseau

Vous pouvez échanger à chaud un module de réseau contre un nouveau module du même type sans avoir à recharger. Cependant, vous devez arrêter le module actuel pour le retirer en toute sécurité. Cette procédure décrit comment arrêter l'ancien module, installer un nouveau module et l'activer.

Pour la mise en grappe ou le basculement, vous ne pouvez pas désactiver un module de réseau si la liaison de commande de grappe ou de basculement se trouve sur le module.

Procédure

Étape 1 Pour la mise en grappe ou le basculement, procédez comme suit :

- **Mise en grappe** : assurez-vous que l'unité sur laquelle vous souhaitez effectuer l'échange à chaud est un nœud de données (voir Modifier le nœud de contrôle, à la page 413); puis désactivez la mise en grappe sur le nœud. Reportez-vous aux sections Devenir un nœud inactif, à la page 409 ou Désactiver un nœud de données du nœud de contrôle, à la page 410.

  Si la liaison de commande de grappe se trouve sur le module de réseau, vous devez quitter la grappe. Consultez Quitter la grappe, à la page 412. La désactivation du module de réseau avec une liaison de commande de grappe active n'est pas autorisée.

- **Basculement** : assurez-vous que l'unité sur laquelle vous souhaitez effectuer l'échange à chaud est le nœud de secours. Consultez Forcer le basculement, à la page 336.

  Si la liaison de basculement se trouve sur le module de réseau, vous devez désactiver le basculement. Consultez Désactiver le basculement, à la page 337. La désactivation du module de réseau avec une liaison de basculement actif n'est pas autorisée.

Étape 2 Désactivez le module de réseau en choisissant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM** et en cochant **Disable Netmod** (Désactiver Netmod).

Étape 3 Cliquez sur **Apply** (Appliquer).

La configuration est appliquée au pare-feu.

Étape 4 Remplacez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez remplacer le module de réseau lorsque le pare-feu est sous tension.

Étape 5 Activez le module de réseau en choisissant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM** et en décochant **Disable Netmod** (Désactiver Netmod).

Étape 6 Cliquez sur **Apply** (Appliquer).

La configuration est appliquée au pare-feu.

Étape 7 Pour la mise en grappe ou le basculement, procédez comme suit :

- Mise en grappe : **rajoutez** le nœud à la grappe. Consultez Rejoindre la grappe, à la page 411 ou Ajouter un nouveau nœud de données à partir du nœud de contrôle, à la page 408.
- **Basculement** : si vous avez désactivé le basculement, veuillez le reconfigurer.

Remplacer le module de réseau par un module de type différent

Si vous remplacez un module de réseau par un autre type, un rechargement est nécessaire. Si le nouveau module comporte moins d'interfaces que l'ancien module, vous devrez supprimer manuellement toute configuration liée aux interfaces qui ne seront plus présentes. Pour la mise en grappe ou le basculement, aucun temps d'arrêt n'est pris en charge. Veuillez donc vous assurer d'effectuer cette procédure pendant une fenêtre de maintenance.

Procédure

Étape 1 Désactivez le module de réseau en choisissant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM** et en cochant **Disable Netmod** (Désactiver Netmod).

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds.

Étape 2 Cliquez sur **Apply** (Appliquer).

La configuration est appliquée au pare-feu. N'enregistrez pas la configuration; lors du rechargement, le module sera activé à l'aide de la configuration enregistrée.

Étape 3 Remplacez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez remplacer le module de réseau lorsque le pare-feu est sous tension.

Pour la mise en grappe ou le basculement, installez le module de réseau sur tous les nœuds.

Étape 4 Rechargez le pare-feu; consultez **Tools (Outils) > System Reload (Rechargement du système)**.

Pour la mise en grappe ou le basculement, rechargez tous les nœuds. Étant donné que les nœuds dotés de modules de réseau différents ne peuvent pas rejoindre la paire de grappe/basculement, vous devez recharger tous les nœuds avec le nouveau module avant qu'ils puissent reformer la paire de grappe/basculement.

Étape 5 Si vous avez enregistré la configuration avant le rechargement, vous devrez réactiver le module.

Retirer le module de réseau

Si vous souhaitez retirer définitivement le module de réseau, procédez comme suit. Le retrait d'un module de réseau nécessite un rechargement. Pour la mise en grappe ou le basculement, aucun temps d'arrêt n'est pris en charge. Veuillez donc vous assurer d'effectuer cette procédure pendant une fenêtre de maintenance.

Avant de commencer

Pour la mise en grappe ou le basculement, assurez-vous que la liaison de basculement ne se trouve pas sur le module de réseau; dans ce cas, vous ne pouvez pas retirer le module.

Procédure

Étape 1 Désactivez le module de réseau en choisissant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM** et en cochant **Disable Netmod** (Désactiver Netmod).

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds.

Étape 2 Cliquez sur **Apply** (Appliquer), puis sur **Save** (Enregistrer).

La configuration est enregistrée sur le pare-feu.

Étape 3 Retirez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez retirer le module de réseau lorsque le pare-feu est sous tension.

Pour la mise en grappe ou le basculement, retirez le module de réseau sur tous les nœuds.

Étape 4 Rechargez le pare-feu; consultez **Tools (Outils) > System Reload (Rechargement du système)**.

Pour la mise en grappe ou le basculement, rechargez tous les nœuds. Étant donné que les nœuds dotés de modules de réseau différents ne peuvent pas rejoindre la paire de grappe/basculement, vous devez recharger tous les nœuds sans le module avant qu'ils puissent reformer la paire de grappe/basculement.

Exemples d'interfaces de base

Consultez les exemples de configuration suivants.

Exemple de paramètres d'interface physique

L'exemple suivant configure les paramètres de l'interface physique en mode unique :

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

Exemple de mode de contexte multiple

L'exemple suivant configure les paramètres d'interface en mode de contexte multiple pour la configuration système et attribue la sous-interface gigabitEthernet 0/1.1 à contexteA :

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

Historique de la configuration de l'interface de base

Tableau 27 : Historique des interfaces

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
La correction d'erreur par défaut (FEC) sur les ports fixes du Secure Firewall 3100 est passée de cl74-fc à cl108-rs pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+.	9.18(3)/9.19(1)	Lorsque vous définissez le FEC sur Auto sur les ports fixes du Secure Firewall 3100, le type par défaut est désormais défini sur cl108-rs au lieu de cl74-fc pour les émetteurs-récepteurs SR, CSR et LR de 25 Go. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Edit Interface (éditer l'interface)** > **Configure Hardware Properties (configurer les propriétés du matériel)** > **FEC Mode (mode FEC)**
Mettre en pause les trames pour le contrôle de flux sur Cisco Secure Firewall 3100	9.18(1)	S'il y a une rafale de trafic, des paquets abandonnés peuvent se produire si la rafale dépasse la capacité de mise en mémoire tampon de la mémoire tampon FIFO sur la carte réseau et les mémoires tampons des anneaux de réception. L'activation des trames de pause pour le contrôle de flux peut atténuer ce problème. Écrans nouveaux ou modifiés : **Configuration** > **Device Settings (Paramètres de l'appareil)** > **Interfaces** > **General (Général)**
Ports d'éclatement pour Secure Firewall 3130 et 3140	9.18(1)	Vous pouvez maintenant configurer quatre ports d'éclatement de 10 Go pour chaque interface de 40 Go sur les Cisco Secure Firewall 3130 et 3140. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de l'échange à chaud du module de réseau pour Secure Firewall 3100	9.17(1)	Vous pouvez ajouter ou retirer le module de réseau sur le pare-feu Secure Firewall 3100 lorsque le pare-feu est sous tension. Pour remplacer un module par un autre module du même type, vous n'avez pas besoin de redémarrer. Après le démarrage initial, l'ajout d'un module, le retrait permanent d'un module ou le remplacement d'un module par un nouveau type nécessite un redémarrage. Écrans Nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM**
Prise en charge de la correction d'erreurs sans voie de retour pour Cisco Secure Firewall 3100	9.17(1)	Les interfaces de Cisco Secure Firewall 3100 25 Gbit/s prennent en charge la correction d'erreurs sans voie de retour (FEC). La FEC est activée par défaut et définie sur Auto. Écrans Nouveaux ou modifiés : **Configuration** > **Device Settings (Paramètres de l'appareil)** > **Interfaces** > **Edit Interface (Modifier l'interface)** > **Configure Hardware Properties (Configurer les propriétés du matériel)**
Prise en charge du réglage de la vitesse en fonction du SFP pour Secure Firewall 3100	9.17(1)	Le pare-feu Secure Firewall 3100 prend en charge la détection de la vitesse pour les interfaces basées sur SFP installées. La détection de SFP est activée par défaut. Cette option est utile si vous modifiez ultérieurement le module de réseau pour un modèle différent et que vous souhaitez que la vitesse se mette à niveau automatiquement. Écrans Nouveaux ou modifiés : **Configuration** > **Device Settings (Paramètres de l'appareil)** > **Interfaces** > **Edit Interface (Modifier l'interface)** > **Configure Hardware Properties (Configurer les propriétés du matériel)**
La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée pour les interfaces de 1 Gigabit et les versions ultérieures.	9.17(1)	La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée séparément de la vitesse pour les interfaces de 1 Gigabit et les versions ultérieures. Écrans Nouveaux ou modifiés : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Advanced (Avancé)**
La négociation automatique de la vitesse peut être désactivée sur les interfaces à fibre optique sur les périphériques Firepower 1100 et 2100.	9.14(1)	Vous pouvez maintenant configurer une interface à fibre optique Firepower 1100 ou 2100 pour désactiver la négociation automatique. Pour les interfaces de 10 Go, vous pouvez configurer la vitesse à 1 Go sans négociation automatique; vous ne pouvez pas désactiver la négociation automatique pour une interface dont la vitesse est réglée à 10 Go. Écrans nouveaux ou modifiés : **Configuration** > **Device Settings (Paramètres de l'appareil)** > **Interfaces** > **Edit Interface (Modifier l'interface)** > **Configure Hardware Properties (Configurer les propriétés du matériel)** > **Speed (Vitesse)**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge du trafic de transit sur l'interface de gestion Management 0/0 pour l'ASA virtuel	9.6(2)	Vous pouvez maintenant autoriser le trafic de transit sur l'interface de gestion Management 0/0 sur l'ASA virtuel. Auparavant, seul l'ASA virtuel sur Microsoft Azure prenait en charge le trafic de transit; maintenant, tous les ASA virtuel le prennent en charge. Vous pouvez éventuellement configurer cette interface pour qu'elle soit en gestion uniquement, mais elle n'est pas configurée par défaut.
Prise en charge des trames de pause pour le contrôle de flux sur les interfaces Gigabit Ethernet	8.2(5)/8.4(2)	Vous pouvez maintenant activer des trames de pause (XOFF) pour le contrôle de flux des interfaces Gigabit Ethernet sur tous les modèles ASA. Nous avons modifié les écrans suivants : (Mode unique) Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier une interface) > General (Général) (Mode multiple, système) Configuration > Interfaces > Add/Edit Interface (Ajouter/modifier une interface).
Prise en charge des trames de pause pour le contrôle de flux sur les interfaces ASA 5580 10 Gigabit Ethernet	8.2(2)	Vous pouvez maintenant activer des trames de pause (XOFF) pour le contrôle de flux. Cette fonctionnalité est également prise en charge sur l'ASA 5585-X. Nous avons modifié les écrans suivants : (Mode unique) Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier une interface) > General (Général) (Mode multiple, système) Configuration > Interfaces > Add/Edit Interface (Ajouter/modifier une interface).
Prise en charge des paquets étendus pour l'ASA 5580	8.1(1)	L'ASA 5580 prend en charge les bâtis grand format. Une trame étendue est un paquet Ethernet supérieur au maximum standard de 1 518 octets (y compris l'en-tête de couche 2 et FCS) qui peut s'élever jusqu'à 9 216 octets. Vous pouvez activer la prise en charge des trames étendues pour toutes les interfaces en augmentant la quantité de mémoire nécessaire pour traiter les trames Ethernet. L'attribution de plus de mémoire aux trames étendues peut limiter l'utilisation maximale d'autres fonctionnalités, telles que les listes de contrôle d'accès. Cette fonctionnalité est également prise en charge sur l'ASA 5585-X. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier une interface) > Advanced (Avancé).

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de Gigabit Ethernet pour la licence Security Plus sur l'ASA 5510	7.2(3)	L'ASA 5510 prend désormais en charge GE (Gigabit Ethernet) pour les ports 0 et 1 avec la licence Security Plus. Si vous mettez à niveau la licence de base vers Security Plus, la capacité des ports Ethernet0/0 et Ethernet0/1 externes passe de FE (Fast Ethernet) (100 Mbps) à GE (1 000 Mbps). Les noms d'interface resteront Ethernet 0/0 et Ethernet 0/1.
Augmentation du nombre d'interfaces pour la licence de base sur l'ASA 5510	7.2(2)	Pour la licence de base sur l'ASA 5510, le nombre maximum d'interfaces est passé de 3 plus une interface de gestion à un nombre illimité d'interfaces.



CHAPITRE 16

Configuration de base de l'interface pour les ports de commutation du Firepower 1010

Vous pouvez configurer chaque interface Firepower 1010 pour qu'elle fonctionne comme une interface pare-feu normale ou comme un port de commutateur matériel de couche 2. Ce chapitre comprend les tâches de démarrage de la configuration de votre port de commutation, notamment l'activation ou la désactivation du mode de commutation, la création d'interfaces VLAN et l'affectation des ports de commutation aux réseaux VLAN. Ce chapitre décrit également comment personnaliser l'alimentation par Ethernet (PoE) sur les interfaces prises en charge.

- À propos des ports de commutation, à la page 629
- Préalables pour les ports de commutation, à la page 630
- Lignes directrices relatives aux ports de commutation, à la page 631
- Configuration des ports de commutation et l'alimentation par Ethernet (PoE), à la page 632
- Supervision des ports de commutation, à la page 637
- Historique des ports de commutation, à la page 638

À propos des ports de commutation

Cette section décrit les ports de commutation pour les modèles avec commutateurs de couche 2.

Comprendre les ports et les interfaces de commutation

Ports et interfaces

Pour chaque interface physique, vous pouvez définir son fonctionnement comme interface de pare-feu ou comme port de commutation. Consultez les renseignements suivants sur les interfaces physiques et les types de port, ainsi que sur les interfaces VLAN logiques auxquelles vous affectez des ports de commutation :

- Interface de pare-feu physique : En mode routé, ces interfaces transmettent le trafic entre les réseaux de la couche 3 en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu et VPN. En mode transparent, ces interfaces sont des membres de groupes de ponts qui acheminent le trafic entre les interfaces du même réseau au niveau de la couche 2, en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu. En mode routé, vous pouvez également utiliser le routage et le pont intégrés avec certaines interfaces comme membres du groupe de ponts et d'autres comme interfaces de couche 3. Par défaut, l'interface Ethernet 1/1 est configurée comme interface de pare-feu.

- Port de commutation physique : les ports de commutation transfèrent le trafic à la couche 2 en utilisant la fonction de commutation dans le matériel. Les ports de commutation sur le même VLAN peuvent communiquer entre eux grâce à la commutation matérielle, et le trafic n'est pas soumis à la politique de sécurité ASA. Les ports d'accès acceptent uniquement le trafic non balisé et vous pouvez les affecter à un seul VLAN. Les ports de ligne principale acceptent le trafic non balisé et peuvent appartenir à plus d'un VLAN. Par défaut, Ethernet 1/2 et supérieur sont configurés comme ports de commutation d'accès sur le VLAN 1. Vous ne pouvez pas configurer l'interface Management (gestion) comme port de commutation.
- Logical VLAN interface (interface VLAN logique) : Ces interfaces fonctionnent de la même façon que les interfaces de pare-feu physiques, à la différence que vous ne pouvez pas créer des sous-interfaces, des , des ou des interfaces EtherChannel. Lorsqu'un port de commutation doit communiquer avec un autre réseau, le périphérique ASA applique la politique de sécurité à l'interface VLAN et achemine le routage vers une autre interface VLAN logique ou une interface de pare-feu. Vous pouvez même utiliser le routage et le pont intégrés avec des interfaces VLAN comme membres du groupe de ponts. Le trafic entre les ports de commutation sur le même VLAN n'est pas soumis à la politique de sécurité, mais le trafic entre les VLAN d'un groupe de ponts est soumis à la politique de sécurité ASA. Vous pouvez donc choisir de superposer les groupes de ponts et les ports de commutation pour appliquer la politique de sécurité entre certains segments.

Alimentation par Ethernet

La PoE est disponible sur Ethernet 1/7 et Ethernet 1/8 en utilisant les protocoles IEEE 802.3af (PoE) et 802.3at (PoE+), jusqu'à 30 W par port.

PoE+ utilise le protocole LLDP (Link Layer Discovery Protocol) pour négocier le niveau de puissance. L'alimentation n'est fournie qu'en cas de besoin.

Si vous désactivez l'interface, vous désactivez l'alimentation du périphérique.

Fonctionnalité Auto-MDI/MDIX

Pour tous les ports de commutation, le paramètre de négociation automatique par défaut inclut également la fonction Auto-MDI/MDIX. La fonction Auto-MDI/MDIX élimine le besoin de câblage croisé en effectuant un croisé interne lorsqu'un câble droit est détecté pendant la phase de négociation automatique. La vitesse ou le duplex doivent être réglés pour qu'ils soient négociés automatiquement afin d'activer Auto-MDI/MDIX pour l'interface. Si vous définissez explicitement la vitesse et le duplex à une valeur fixe, désactivant ainsi la négociation automatique pour les deux paramètres, Auto-MDI/MDIX est également désactivé. Lorsque la vitesse et le mode duplex sont définis à 1000 et que la vitesse maximale est atteinte, l'interface négocie toujours automatiquement; par conséquent, Auto-MDI/MDIX est toujours activé et vous ne pouvez pas le désactiver.

Préalables pour les ports de commutation

Prise en charge des modèles

- Firepower 1010

Lignes directrices relatives aux ports de commutation

Mode contextuel

- Firepower 1010 ne prend pas en charge le mode contexte multiple.
- Le Secure Firewall 1210/1220 ne prend pas en charge le mode de contexte multiple.

Basculement et mise en grappe

- Aucune prise en charge de grappe.
- Prise en charge du basculement actif/veille uniquement.
- Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l'utilisation de Basculement. Étant donné que les ports de commutation fonctionnent dans le matériel, ils continuent de faire circuler le trafic sur les unités actives *et* en veille. Basculement est conçu pour empêcher le trafic de passer par l'unité en veille, mais cette fonctionnalité ne s'étend pas aux ports de commutation. Dans une configuration réseau Basculement normale, les ports de commutateur actifs sur les deux unités mèneront à des boucles réseau. Nous vous suggérons d'utiliser des commutateurs externes pour toute capacité de commutation. Notez que les interfaces VLAN peuvent être surveillées par basculement, contrairement aux ports de commutation. Théoriquement, vous pouvez mettre un port de commutation unique sur un réseau VLAN et utiliser Basculement avec succès, mais une configuration plus simple consiste à utiliser des interfaces physiques de pare-feu à la place.
- Vous ne pouvez utiliser qu'une interface de pare-feu comme liaison de basculement.

Interfaces logiques VLAN (SVI)

- Si vous utilisez également des sous-interfaces VLAN sur une interface de pare-feu, vous ne pouvez pas utiliser le même ID VLAN que pour une interface VLAN logique.
- Adresses MAC
  - Mode de pare-feu routé : toutes les interfaces VLAN partagent une adresse MAC. Assurez-vous que tous les commutateurs connectés peuvent prendre en charge ce scénario. Si les commutateurs connectés nécessitent des adresses MAC uniques, vous pouvez attribuer manuellement des adresses MAC. Consultez Configurer l'adresse MAC manuelle, la MTU et le TCP MSS, à la page 737
  - Mode pare-feu transparent : chaque interface VLAN a une adresse MAC unique. Vous pouvez remplacer les adresses MAC générées si vous le souhaitez en attribuant manuellement des adresses MAC. Consultez Configurer l'adresse MAC manuelle, la MTU et le TCP MSS, à la page 737.

Groupes de ponts

Vous ne pouvez pas mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques dans le même groupe de ponts.

Fonctionnalités non prises en charge de l'interface VLAN et du port de commutation

Les interfaces VLAN et les ports de commutation ne prennent pas en charge :

- Routage dynamique
- Routage multidiffusion
- Routage basé sur les politiques
- Routage multiples chemins à coûts égaux (ECMP)
- VXLAN
- EtherChannels : les ports de commutation ne peuvent pas faire partie d'un EtherChannel. Le PoE n'est pas non plus pris en charge sur un port d'un EtherChannel.
- Basculement et lien d'état
- Zones de circulation
- Balise du groupe de sécurité (SGT)

Autres directives et limites

- Vous pouvez configurer un maximum de 60 interfaces nommées.
- Vous ne pouvez pas configurer l'interface Management (gestion) comme port de commutation.

Paramètres d'usine

- Ethernet 1/1 est une interface de pare-feu.
- Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.
- Vitesse et duplex par défaut: par défaut, la vitesse et le duplex sont configurés pour la négociation automatique.

Configuration des ports de commutation et l'alimentation par Ethernet (PoE)

Pour configurer les ports de commutation et la PoE, procédez comme suit :

Configurer une interface VLAN

Cette section décrit comment configurer les interfaces VLAN (SVI) à utiliser avec les ports de commutation associés. Vous pouvez créer jusqu'à 60 interfaces VLAN associées aux ports de commutation.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres de l'interface)** > **Interfaces** et choisissez **Add (Ajouter)** > **VLAN Interface (Interface VLAN)**.

Étape 2 Dans le champ **VLAN ID** (ID de VLAN), saisissez l'ID de VLAN pour cette interface, entre 1 et 4070, en excluant les ID de 3968 à 4047, qui sont réservés à un usage interne.

Étape 3 (Facultatif) Dans la liste déroulante **Block Traffic From this Interface to** (Bloquer le trafic de cette interface à), choisissez le VLAN vers lequel cette interface VLAN ne peut pas initier le trafic.

Par exemple, vous avez un VLAN affecté à l'extérieur pour l'accès Internet, un VLAN affecté à un réseau interne d'entreprise et un troisième VLAN affecté à votre réseau domestique. Le réseau domestique n'a pas besoin d'accéder au réseau de l'entreprise, vous pouvez donc utiliser l'option **Block Traffic From this Interface to** (Bloquer le trafic de cette interface à) sur le VLAN domestique; le réseau professionnel peut accéder au réseau domestique, mais le réseau domestique ne peut pas accéder au réseau d'entreprise.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Apply** (Appliquer).

Configuration des ports de commutation comme ports d'accès

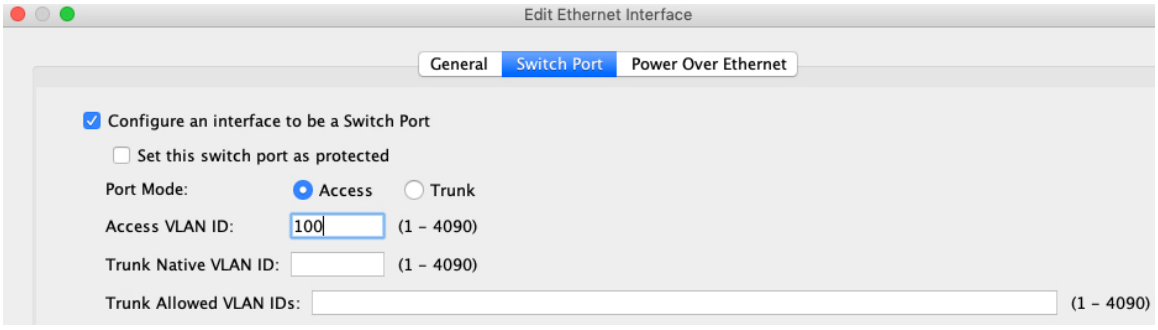
Pour affecter un port de commutation à un seul VLAN, configurez-le comme port d'accès. Les ports d'accès acceptent uniquement le trafic non balisé. Par défaut, Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.

Remarque L'appareil ne prend pas en charge le protocole Spanning Tree pour la détection de boucle dans le réseau. Par conséquent, vous devez vous assurer qu'une connexion avec l'ASA ne finit pas dans une boucle de réseau.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, sélectionnez l'interface que vous souhaitez modifier et cliquez sur **Edit** (Modifier).

Étape 2 Cliquez sur **Switch Port** (Port de commutation).



Étape 3 Cochez la case **Configure an interface to be a Switch Port** (Configurer une interface pour qu'elle soit un port de commutation).

Étape 4 (Facultatif) Cochez la case **Set this switch port as protected** (Définir ce port de commutation comme protégé) pour définir ce port de commutation comme protégé, afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres en appliquant l'option **Set this switch port as protected** (Définir ce port de commutation comme protégé) à chaque port de commutation. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

Étape 5 Pour le **Port Mode** (Mode de port), cliquez sur le bouton radio **Access** (Accès).

Étape 6 Saisissez l'**Access VLAN ID** (ID de VLAN d'accès) associé à ce port de commutation, entre 1 et 4070.

La valeur par défaut est VLAN 1.

Étape 7 Cliquez sur **General** (Général).

Étape 8 Cochez **Enable Interface** (Activer l'interface).



Remarque Les autres champs de la page **General** (Général), comme **Interface Name** (Nom de l'interface), ne s'appliquent pas aux ports de commutation.

Étape 9 (Facultatif) Définissez les propriétés matérielles.

a) Cliquez sur **Configure Hardware Properties** (Configurer les propriétés matérielles).

b) Choisissez le mode **Duplex**.

La valeur par défaut est **Auto**.

c) Renseignez le champ **Speed** (Vitesse).

La valeur par défaut est **Auto**.

d) Cliquez sur **OK**.

Étape 10 Cliquez sur **OK**.

Étape 11 Cliquez sur **Apply** (Appliquer).

Configuration des ports de commutation comme ports de ligne principale

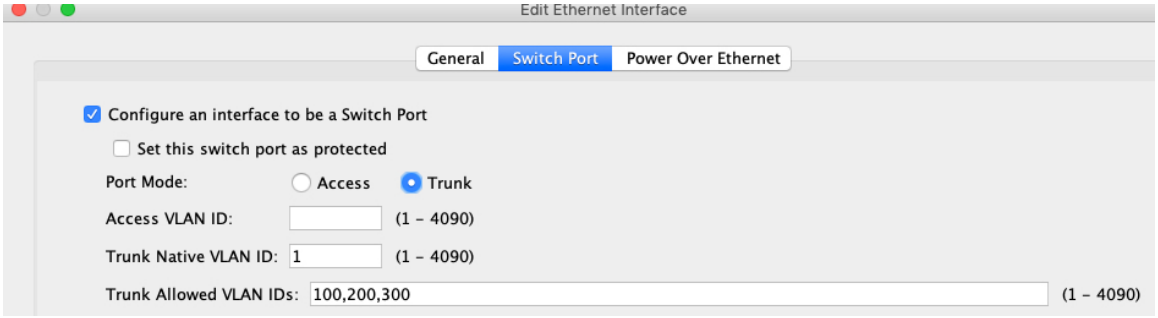
Cette procédure décrit comment créer un port de liaison qui peut acheminer plusieurs VLAN à l'aide du balisage 802.1Q. Les ports de ligne principale acceptent le trafic non balisé et balisé. Le trafic sur les VLAN autorisés passe par le port de liaison sans changement.

Lorsque la ligne principale reçoit un trafic non balisé, elle le balise à l'ID de VLAN natif afin que l'ASA puisse transférer le trafic vers les ports de commutation appropriés ou l'acheminer vers une autre interface de pare-feu. Lorsque l'ASA envoie le trafic d'ID de VLAN natif hors du port de liaison, il supprime la balise VLAN. Assurez-vous de définir le même VLAN natif sur le port de liaison de l'autre commutateur afin que le trafic non balisé soit balisé vers le même VLAN.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, sélectionnez l'interface que vous souhaitez modifier et cliquez sur **Edit** (Modifier).

Étape 2 Cliquez sur **Switch Port** (Port de commutation).



Étape 3 Cochez la case **Configure an interface to be a Switch Port** (Configurer une interface pour qu'elle soit un port de commutation).

Étape 4 (Facultatif) Cochez la case **Set this switch port as protected** (Définir ce port de commutation comme protégé) pour définir ce port de commutation comme protégé, afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres en appliquant l'option **Set this switch port as protected** (Définir ce port de commutation comme protégé) à chaque port de commutation. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

Étape 5 Pour le **Port Mode** (Mode de port), cliquez sur le bouton radio **Trunk** (Liaison).

Étape 6 Saisissez le **Trunk Native VLAN ID** (ID de VLAN natif de la liaison), compris entre 1 et 4070. La valeur par défaut est VLAN 1.

Chaque port ne peut avoir qu'un seul VLAN natif, mais chaque port peut avoir le même VLAN natif ou un différent.

Étape 7 Saisissez les **Trunk Allowed VLAN IDs** (ID de VLAN autorisés pour la liaison) associés à ce port de commutation, séparés par des virgules, entre 1 et 4070.

Si vous incluez le VLAN natif dans ce champ, il est ignoré; Le port de liaison supprime toujours le balisage VLAN lors de l'envoi de trafic VLAN natif hors du port. De plus, il ne recevra pas le trafic qui a toujours un balisage VLAN natif.

Étape 8 Cliquez sur **General** (Général).

Étape 9 Cochez **Enable Interface** (Activer l'interface).

Remarque Les autres champs de la page **General** (Général), comme **Interface Name** (Nom de l'interface), ne s'appliquent pas aux ports de commutation.

Étape 10 (Facultatif) Définissez les propriétés matérielles.

a) Cliquez sur **Configure Hardware Properties** (Configurer les propriétés matérielles).

b) Choisissez le mode **Duplex**.

La valeur par défaut est **Auto**.

c) Renseignez le champ **Speed** (Vitesse).

La valeur par défaut est **Auto**.

d) Cliquez sur **OK**.

Étape 11 Cliquez sur **OK**.

Étape 12 Cliquez sur **Apply** (Appliquer).

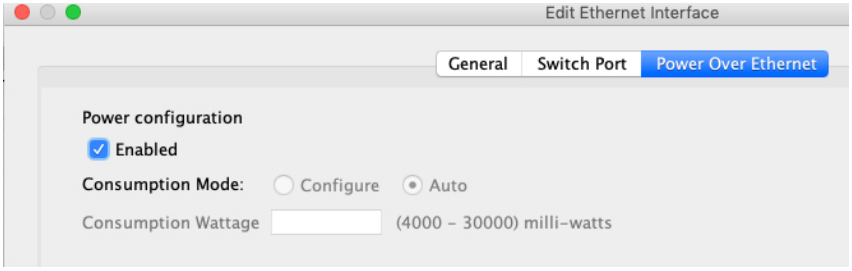
Configurer Power Over Ethernet (alimentation électrique par câble Ethernet)

Les ports Power over Ethernet (PoE) alimentent les périphériques tels que les téléphones IP ou les points d'accès sans fil. Le mode PoE est activé par défaut. Cette procédure décrit comment activer et désactiver la PoE et comment définir les paramètres facultatifs.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, sélectionnez l'interface que vous souhaitez modifier et cliquez sur **Edit** (Modifier).

Étape 2 Cliquez sur **Power Over Ethernet** (Alimentation par Ethernet).



Étape 3 Cochez la case **Activé**.

Étape 4 Cliquez sur le bouton radio **Consumption Mode** (Mode de consommation) : **Configure** (Configurer) ou **Auto**.

- **Auto** : fournit automatiquement du courant au périphérique alimenté en utilisant une puissance appropriée pour la classe du périphérique alimenté. Le pare-feu utilise LLDP pour négocier davantage la puissance en watts.

- **Configure** (Configurer) : spécifie manuellement la puissance en milliwatts dans le champ **Consumption Wattage** (Consommation en watts), de 4 000 à 30 000. Utilisez cette option si vous souhaitez définir les watts manuellement et désactiver la négociation LLDP.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** (Appliquer).

Étape 7 Choisissez **Monitor (Superviser)** > **Interfaces** > **Power Over Ethernet (Alimentation par Ethernet)** pour afficher l'état PoE actuel.

Supervision des ports de commutation

- **Monitoring (Supervision)** > **Interfaces** > **ARP Table (Tableau ARP)**

  Affiche le tableau ARP, y compris les entrées statiques et dynamiques. Le tableau ARP comprend des entrées qui mappent une adresse MAC à une adresse IP pour une interface donnée.

- **Monitoring (Supervision)** > **Interfaces** > **MAC Address Table (Tableau d'adresses MAC)**

  Affiche les entrées d'adresse MAC statiques et dynamiques.

- **Monitoring (Supervision)** > **Interfaces** > **Interface Graphs (Graphiques d'interface)**

  Affiche les statistiques d'interface sous forme de graphique ou de tableau.

- **Monitoring (Supervision)** > **Interfaces** > **L2 Switching (Commutation L2)**

  Affiche l'association du port VLAN au commutateur et les entrées d'adresses MAC statiques et dynamiques.

- **Monitoring (Supervision)** > **Interfaces** > **Power Over Ethernet (Alimentation par Ethernet)**

  Affiche l'état PoE+.

Historique des ports de commutation

Tableau 28 : Historique des ports de commutation

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge du commutateur matériel Firepower 1010	9.13(1)	L'appareil Firepower 1010 prend en charge la définition de chaque interface Ethernet comme port de commutation ou interface de pare-feu. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Edit (Modifier)** > **Switch Port (Port de commutation)** • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add VLAN Interface (Ajouter une interface VLAN)** • **Monitoring (Supervision)** > **Interfaces** > **L2 Switching (Commutation L2)**
Prise en charge du Firepower 1010 PoE+ sur Ethernet 1/7 et Ethernet 1/8	9.13(1)	Le Firepower 1010 prend en charge Power over Ethernet+ (PoE+) sur Ethernet 1/7 et Ethernet 1/8. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Edit (Modifier)** > **Power Over Ethernet (Alimentation par Ethernet)** • **Monitoring (Supervision)** > **Interfaces** > **Power Over Ethernet (Alimentation par Ethernet)**



CHAPITRE 17

Interfaces EtherChannel

Ce chapitre explique comment configurer les EtherChannels.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà dans l'espace d'exécution système, dans le volet **Configuration** > **Device List** (Liste des périphériques), double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Pour les interfaces de grappe ASA, qui ont des exigences spéciales, consultez Grappe ASA pour le Secure Firewall 3100, à la page 363.

Remarque Pour Firepower 2100 en mode plateforme et Châssis Firepower 4100/9300 , les interfaces EtherChannel sont configurées dans le système d'exploitation FXOS. Consultez le guide de configuration ou de démarrage de votre châssis pour en savoir plus.

- À propos des EtherChannels, à la page 639
- Directives pour les EtherChannels, à la page 643
- Paramètres par défaut pour les interfaces EtherChannels, à la page 645
- Configurer un EtherChannel , à la page 646
- Exemples d'EtherChannels, à la page 650
- Historique des EtherChannels, à la page 650

À propos des EtherChannels

La présente section décrit les canaux EtherChannels.

About EtherChannels

Un EtherChannel 802.3ad est une interface logique (appelée interface de canal de port) composée d'un ensemble de liaisons Ethernet individuelles (un groupe de canaux), ce qui vous permet d'augmenter la bande passante pour un seul réseau. Une interface de canal de port est utilisée de la même manière qu'une interface physique lorsque vous configurez les fonctionnalités liées à l'interface.

Vous pouvez configurer jusqu'à 48 EtherChannels, selon le nombre d'interfaces prises en charge par votre modèle.

Interfaces des groupes de canaux

Chaque groupe de canaux peut avoir jusqu'à 8 interfaces actives, sauf pour ASA, les l'ISA 3000, qui prend en charge 16 interfaces actives. Pour les commutateurs qui prennent en charge seulement 8 interfaces actives, vous pouvez affecter jusqu'à 16 interfaces à un groupe de canaux : alors que seules 8 interfaces peuvent être actives, les interfaces restantes peuvent servir de liaisons de secours en cas de défaillance de l'interface.

Toutes les interfaces du groupe de canaux doivent être du même type et de la même vitesse. La première interface ajoutée au groupe de canaux détermine le type et la vitesse à respecter.

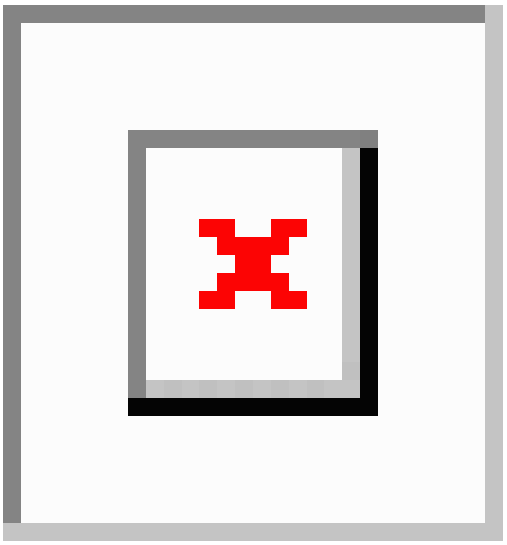
L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal. L'interface est sélectionnée à l'aide d'un algorithme de hachage exclusif, en fonction des adresses MAC source ou de destination, des adresses IP, des numéros de ports TCP et UDP et des numéros de VLAN.

Connexion à un EtherChannel sur un autre périphérique

Le périphérique auquel vous connectez l'EtherChannel ASA doit également prendre en charge l'EtherChannel 802.3ad; par exemple, vous pouvez vous connecter au commutateur Catalyst 6500 ou à Cisco Nexus 7000.

Lorsque le commutateur fait partie d'un système de commutation virtuelle (VSS) ou d'un canal de port virtuel (vPC), vous pouvez connecter des interfaces ASA dans le même EtherChannel pour séparer les commutateurs dans le VSS/vPC. Les interfaces des commutateurs sont membres de la même interface de canal de port EtherChannel, car les commutateurs distincts se comportent comme un seul commutateur.

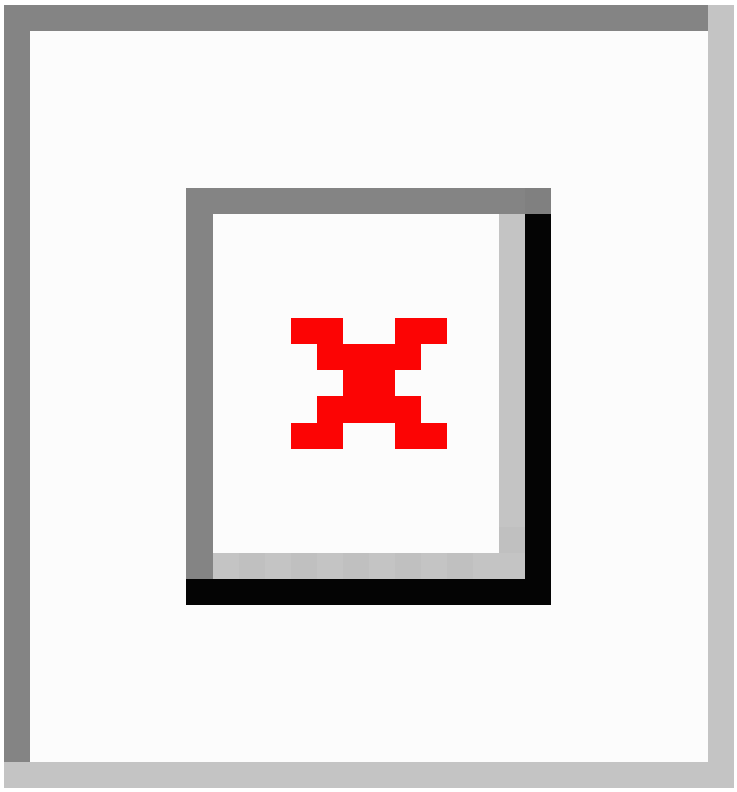
Illustration 70 : Connexion à un VSS/vPC



Remarque Si le périphérique ASA est en mode de pare-feu transparent et que vous placez le périphérique ASA entre deux ensembles de commutateurs VSS/vPC, veillez à désactiver la détection unidirectionnelle de liaison (UDLD) sur tous les ports de commutateur connectés au périphérique ASA avec un EtherChannel. Si vous activez UDLD, un port de commutation peut recevoir des paquets UDLD provenant des deux commutateurs de l'autre paire VSS/vPC. Le commutateur de réception place l'interface de réception à l'état inactif avec la raison « UDLD Neighbor mismatch » (Mauvaise correspondance des voisins UDLD).

Si vous utilisez le périphérique ASA dans un déploiement de basculement actif/en veille, vous devez créer des EtherChannels distincts sur les commutateurs du VSS/vPC, un pour chaque périphérique ASA. Sur chaque périphérique ASA, un seul EtherChannel se connecte aux deux commutateurs. Même si vous pouviez regrouper toutes les interfaces de commutateur dans un seul EtherChannel qui vous connecte aux deux périphériques ASA (dans ce cas, l'EtherChannel ne sera pas établi en raison des ID de système ASA distincts), un seul EtherChannel ne serait pas souhaitable, car vous ne pouvez pas souhaiter que le trafic soit envoyé au périphérique ASA.

Illustration 71 : Basculement actif/en veille et VSS/vPC



Protocole LACP (Link Aggregation Control Protocol)

Le protocole LACP (Link Aggregation Control Protocol) agrège les interfaces en échangeant les LACPDU (Link Aggregation Control Protocol Data Unit) entre deux périphériques réseau.

Vous pouvez configurer chaque interface physique d'un EtherChannel pour qu'elle soit :

- Actif : envoie et reçoit les mises à jour du protocole LACP. Un EtherChannel actif peut établir une connectivité avec un EtherChannel actif ou passif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.
- Passive : reçoit les mises à jour du protocole LACP. Un EtherChannel passif ne peut établir une connectivité qu'avec un EtherChannel actif. Non pris en charge sur les modèles matériel.
- Activé : l'EtherChannel est toujours activé et le protocole LACP n'est pas utilisé. Un EtherChannel « activé » ne peut établir une connexion qu'avec un autre EtherChannel « activé ».

Le protocole LACP coordonne l'ajout et la suppression automatiques des liens vers l'EtherChannel sans l'intervention de l'utilisateur. Il gère également les erreurs de configuration et vérifie que les deux extrémités des interfaces membres sont connectées au groupe de canaux approprié. Le mode « On » ne peut pas utiliser les interfaces en veille dans le groupe de canaux lorsqu'une interface tombe en panne et que la connectivité et les configurations ne sont pas vérifiées.

Équilibrage de la charge

Le périphérique ASA distribue les paquets aux interfaces de l'EtherChannel en hachant l'adresse IP de source et de destination du paquet (ce critère est configurable). Le hachage obtenu est divisé par le nombre de liens actifs dans une opération modulo, le reste déterminant l'interface propriétaire du flux. Tous les paquets avec un résultat *hash_value* **mod** *active_links* de 0 sont dirigés vers la première interface de l'EtherChannel, les paquets avec un résultat de 1 vont à la deuxième interface, les paquets de résultat de 2 à la troisième interface, etc. Par exemple, si vous avez 15 liens actifs, l'opération modulo fournit des valeurs de 0 à 14. Pour six liens actifs, les valeurs sont comprises entre 0 et 5, et ainsi de suite.

Pour un EtherChannel étendu en grappe, l'équilibrage de charge se produit sur une base de l'ASA. Par exemple, s'il y a 32 interfaces actives dans l'EtherChannel sur 8 ASA, avec 4 interfaces par ASA dans l'EtherChannel, l'équilibrage de la charge ne se produit que sur les 4 interfaces du l'ASA.

Si une interface active tombe en panne et n'est pas remplacée par une interface de secours, le trafic est rééquilibrage entre les liaisons restantes. La défaillance est masquée à la fois par le Spanning Tree au niveau de la couche 2 et la table de routage au niveau de la couche 3, de sorte que le basculement est transparent pour les autres périphériques du réseau.

Sujets connexes

Personnaliser l'EtherChannel, à la page 648

Adresse MAC de l'EtherChannel

Toutes les interfaces qui font partie du groupe de canaux partagent la même adresse MAC. Cette fonction rend l'EtherChannel transparent pour les applications et les utilisateurs du réseau, car ils ne voient qu'une seule connexion logique; ils n'ont aucune connaissance des liens individuels.

Matériel Firepower et Cisco Secure Firewall

L'interface du canal de port utilise l'adresse MAC de l'interface interne Internal-Data 0/1. Vous pouvez également configurer manuellement une adresse MAC pour l'interface du canal de port. En mode de contexte multiple, vous pouvez affecter automatiquement des adresses MAC uniques aux interfaces *partagées*, y compris une interface de port EtherChannel. Toutes les interfaces EtherChannel d'un châssis utilisent la même adresse MAC. Sachez donc que si vous utilisez l'interrogation SNMP, par exemple, plusieurs interfaces auront la même adresse MAC.

Remarque Les interfaces membres utilisent l'adresse MAC Internal-Data 0/1 uniquement après un redémarrage. Avant de redémarrer, l'interface membre utilise sa propre adresse MAC. Si vous ajoutez une nouvelle interface membre après un redémarrage, vous devrez effectuer un autre redémarrage pour mettre à jour son adresse MAC.

Directives pour les EtherChannels

Groupe de ponts

En mode routé, les EtherChannels définis par l'ASA ne sont pas pris en charge en tant que membres du groupe de ponts. Les EtherChannels sur le Firepower 4100/9300 peuvent être des membres de groupes de ponts.

Basculement

- Lorsque vous utilisez une interface EtherChannel comme lien Basculement, elle doit être préconfigurée sur les deux unités de la paire Basculement; vous ne pouvez pas le configurer sur l'unité principale et vous attendre à ce qu'il soit dupliquée sur l'unité secondaire, car *le lien Basculement lui-même est requis pour la duplication*.
- Si vous utilisez une interface EtherChannel , aucune configuration particulière n'est requise; la configuration peut être répliquée normalement à partir de l'unité principale. Pour le Châssis Firepower 4100/9300 , toutes les interfaces, y compris l'EtherChannels, doivent être préconfigurées sur les deux unités.
- Vous pouvez surveiller l'EtherChannel pour Basculement. Lorsqu'une interface membre active bascule vers une interface de secours, cette activité ne fait pas apparaître l'EtherChannel comme défaillant lors de la surveillance au niveau du périphérique Basculement. Ce n'est que lorsque toutes les interfaces physiques tombent en panne que l'EtherChannel semble défaillante (pour une interface EtherChannel, le nombre d'interfaces membres autorisées à échouer peut être configuré).
- Si vous utilisez une interface EtherChannel pour un Basculement ou une liaison d'état, pour éviter les paquets dans le désordre, une seule interface de l'EtherChannel est utilisée. Si cette interface échoue, l'interface suivante de l'EtherChannel est utilisée. Vous ne pouvez pas modifier la configuration de l'EtherChannel lorsqu'elle est utilisée en tant que lien Basculement. Pour modifier la configuration, vous devez désactiver temporairement Basculement, ce qui empêche Basculement de se produire pendant la durée.

Prise en charge des modèles

- Vous ne pouvez pas ajouter des EtherChannels dans ASA pour le Firepower 2100 en mode plateforme, Firepower 4100/9300 ou l'ASA virtuel. Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis.
- Vous ne pouvez pas utiliser les ports de commutation ni les interfaces VLAN de Firepower 1010 dans les EtherChannels.

Mise en grappe

- Pour configurer un EtherChannel étendu ou une interface de grappe individuelle, consultez le chapitre sur la mise en grappe.

Directives générales EtherChannel

- Vous pouvez configurer jusqu'à 48 EtherChannels, selon le nombre d'interfaces disponibles sur votre modèle.
- Chaque groupe de canaux peut avoir jusqu'à 8 interfaces actives, sauf pour ASA, les l'ISA 3000, qui prend en charge 16 interfaces actives. Pour les commutateurs qui prennent en charge seulement 8 interfaces actives, vous pouvez affecter jusqu'à 16 interfaces à un groupe de canaux : alors que seules 8 interfaces peuvent être actives, les interfaces restantes peuvent servir de liaisons de secours en cas de défaillance de l'interface.
- Lorsque vous ajoutez la première interface membre, elle définit les propriétés matérielles requises de toutes les interfaces membres.
  - Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les interfaces RJ-45 et SFP.
  - Toutes les interfaces doivent être définies à la même vitesse et au même duplex.
  - La première interface définit la *capacité* de vitesse, qui ne peut pas être modifiée ultérieurement.
    - Pour les interfaces de détection SFP : vous pouvez inclure des interfaces avec des capacités de vitesse différentes, tant qu'elles ont une vitesse commune. Lorsque vous définissez la vitesse sur SFP Detect (par défaut), la vitesse est définie dynamiquement à la vitesse commune la plus élevée. Si vous modifiez ultérieurement les interfaces membres de sorte que la vitesse commune soit maintenant plus élevée, la vitesse EtherChannel sera également plus élevée automatiquement.

      Vous pouvez définir une vitesse spécifique, mais uniquement les vitesses disponibles sur la première interface membre. Par exemple, si votre première interface est 1/10 Go, les vitesses disponibles pour l'EtherChannel seront de 1 Go, 10 Go et SFP détecté. Si vous supprimez ultérieurement les interfaces de 1/10 Go et les remplacez par des interfaces de 1/10/25 Go, vous ne pourrez pas définir manuellement la vitesse à 25 Go. Dans ce cas, vous pouvez utiliser SFP Detect pour utiliser la vitesse de 25 Go.
    - Pour les interfaces de détection non SFP : toutes les interfaces supplémentaires doivent avoir la même capacité de vitesse. Par exemple, si la capacité de vitesse de votre première interface est de 10 Mo/100 Mo/1 Go, vous devez ajouter d'autres interfaces de 10 Mo/100 Mo/1 Go. Vous pouvez définir l'EtherChannel (et ses interfaces membres) à n'importe quelle de ces vitesses. Vous ne pouvez pas ajouter ultérieurement d'interfaces de 1/10 Go à l'EtherChannel, même si vous supprimez les interfaces de capacité inférieure. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité.
- Le périphérique auquel vous connectez l'EtherChannel ASA doit également prendre en charge l'EtherChannel 802.3ad.
- Le périphérique ASA ne prend pas en charge les unités LACPDU marquées VLAN. Si vous activez le balisage VLAN natif sur le commutateur voisin à l'aide de la commande Cisco IOS **vlan dot1Q tag native**, le périphérique ASA abandonnera les LACPDU balisées. Assurez-vous de désactiver le balisage

VLAN natif sur le commutateur voisin. En mode de contexte multiple, ces messages ne sont pas inclus dans une capture de paquets, de sorte que vous ne pouvez pas diagnostiquer le problème facilement.

- Le débit LACP dépend du modèle. Lorsque vous définissez le débit (normal ou rapide), l'appareil demande ce débit au commutateur de connexion. En retour, l'appareil enverra au débit demandé par le commutateur de connexion. Nous vous recommandons de définir le même débit des deux côtés.
  - Firepower 4100/9300 : le débit LACP est défini sur rapide par défaut dans FXOS, mais vous pouvez le configurer comme normal (également appelé lent).
  - Secure Firewall 3100 : le débit LACP est défini par défaut sur normal (lent), mais vous pouvez le configurer sur rapide sur l'appareil.
  - Tous les autres modèles : le débit LACP est défini sur normal (également appelé lent) et il n'est pas configurable, ce qui signifie que l'appareil demandera toujours un débit lent au commutateur de connexion. Nous vous recommandons de configurer le taux du commutateur sur « lent » pour que les deux côtés envoient les messages LACP au même rythme.
- Dans les versions du logiciel Cisco IOS antérieures à la 15.1(1)S2, ASA ne prenait pas en charge la connexion d'un EtherChannel à une pile de commutateurs. Avec les paramètres par défaut du commutateur, si l'EtherChannel ASA est connecté en pile croisée, et si le commutateur principal est mis hors tension, l'EtherChannel connecté au commutateur restant ne sera pas mis en service. Pour améliorer la compatibilité, définissez la commande **stack-mac persistent timer** sur une valeur suffisamment grande pour prendre en compte le temps de rechargement; par exemple, 8 minutes ou 0 pour indéfini. Vous pouvez également effectuer une mise à niveau vers une version plus stable du logiciel du commutateur, comme par exemple 15.1(1)S2.
- Toute la configuration ASA fait référence à l'interface logique EtherChannel plutôt qu'aux interfaces physiques membres.

Paramètres par défaut pour les interfaces EtherChannels

Cette section répertorie les paramètres par défaut des interfaces si vous n'avez pas de configuration d'usine par défaut.

État par défaut des interfaces

L'état par défaut d'une interface dépend du type d'interface et du mode de contexte.

En mode de contexte multiple, toutes les interfaces allouées sont activées par défaut, quel que soit l'état de l'interface dans l'espace d'exécution du système. Cependant, pour que le trafic passe par l'interface, celle-ci doit également être activée dans l'espace d'exécution du système. Si vous désactivez une interface dans l'espace d'exécution du système, cette interface est désactivée dans tous les contextes qui la partagent.

En mode unique ou dans l'espace d'exécution du système, les interfaces ont les états par défaut suivants :

- Interfaces physiques : désactivées.
- Interfaces de canal de port EtherChannel — Activées. Cependant, pour que le trafic passe par l'EtherChannel, les interfaces physiques des groupes de canaux doivent également être activées.

Configurer un EtherChannel

Cette section décrit comment créer une interface de canal de port EtherChannel, affecter des interfaces à l'EtherChannel et personnaliser l'EtherChannel.

Ajouter des interfaces à l'EthernetChannel

Cette section décrit comment créer une interface de canal de port EtherChannel et affecter des interfaces à l'EtherChannel. Par défaut, les interfaces de canal de port sont activées.

Avant de commencer

- Lorsque vous ajoutez la première interface membre, elle définit les propriétés matérielles requises de toutes les interfaces membres. Consultez Directives pour les EtherChannels, à la page 643 pour plus de détails sur les exigences des interfaces membres.
- Pour configurer un EtherChannel étendu pour la mise en grappe, consultez le chapitre sur la mise en grappe au lieu de cette procédure.
- Vous ne pouvez pas ajouter d'interface physique au groupe de canaux si vous lui avez configuré un nom. Vous devez d'abord supprimer le nomdans le volet **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces**.
- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà dans le mode de configuration système, dans le volet **Configuration** > **Device List (Liste des périphériques)**, double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Mise en garde Si vous utilisez une interface physique déjà présente dans votre configuration, la suppression du nom effacera toute configuration faisant référence à l'interface.

Procédure

Étape 1 (Facultatif) (Secure Firewall 3100 uniquement) Définissez le débit de réception de l'unité de données LACP pour une interface physique dans le groupe de canaux.

lacp rate {**normal** | **fast**}

La valeur par défaut est de **normal** (lent, toutes les 30 secondes). L'option **fast** reçoit des unités de données LACP chaque seconde. Vous devez faire correspondre le paramètre sur le commutateur connecté.

Étape 2 Selon votre mode de contexte :

- Pour le mode unique, choisissez le volet **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.
- Pour le mode multiple dans l'espace d'exécution du système, choisissez le volet **Configuration** > **Context Management (Gestion des contextes)** > **Interfaces**.

Étape 3 Choisissez **Add** > **EtherChannel Interface** (Ajouter une interface EthernetChannel).

La boîte de dialogue **Add EtherChannel Interface** (Ajouter une interface EtherChannel) apparaît.

Remarque En mode unique, cette procédure ne couvre qu'un sous-ensemble des paramètres de la boîte de dialogue Edit EtherChannel Interface (Modifier une interface EtherChannel). Notez qu'en mode de contexte multiple, avant de terminer la configuration de l'interface, vous devez attribuer des interfaces aux contextes. Consultez Configurer plusieurs contextes, à la page 269.

Étape 4 Dans le champ **Port Channel ID** (ID de canal de port), saisissez un numéro compris entre 1 et 48 (1 et 8 pour les périphériques Firepower 1010).

Étape 5 Dans la zone **Available Physical Interface** (Interface physique disponible), cliquez sur une interface, puis sur **Add** (Ajouter) pour la déplacer vers la zone **Members in Group** (Membres du groupe).

En mode transparent, si vous créez un groupe de canaux avec plusieurs interfaces de gestion, vous pouvez utiliser cet EtherChannel comme interface de gestion uniquement.

Remarque Si vous souhaitez activer le mode EtherChannel, vous ne devez inclure qu'une seule interface au départ. Après avoir terminé cette procédure, modifiez l'interface membre et définissez le mode sur **On** (Activé). Appliquez vos modifications, puis modifiez l'EtherChannel pour ajouter d'autres interfaces membres.

Étape 6 Répétez l'opération pour chaque interface que vous souhaitez ajouter au groupe de canaux.

Vérifiez que toutes les interfaces sont du même type et ont la même vitesse. La première interface que vous ajoutez détermine le type et la vitesse de l'EtherChannel. Toutes les interfaces non correspondantes que vous ajoutez seront mises à l'état suspendu. ASDM ne vous empêche pas d'ajouter des interfaces non correspondantes.

Étape 7 Cliquez sur **OK**.

Vous retournez dans le volet **Interfaces**. Les interfaces membres affichent désormais un cadenas à gauche de l'ID d'interface indiquant que seuls les paramètres de base peuvent être configurés pour celle-ci. L'interface EtherChannel est ajoutée au tableau.



Étape 8 (Facultatif) (Secure Firewall 3100 uniquement) Définissez le débit de réception de l'unité de données LACP pour une interface physique dans le groupe de canaux.

a) Cliquez sur l'interface physique dans le tableau **Interfaces**, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche.

b) Cliquez sur l'onglet **Advanced (Avancé)**.

c) Dans la zone **EtherChannel**, dans la liste déroulante **Rate** (Débit), choisissez **Normal** ou **Fast** (Rapide).

La valeur par défaut est **Normal** (lent, toutes les 30 secondes). L'option **Fast** (Rapide) reçoit des mises à jour LACP chaque seconde. Vous devez faire correspondre le paramètre sur le commutateur connecté.

Étape 9 Cliquez sur **Apply** (Appliquer). Toutes les interfaces membres sont activées automatiquement.

Sujets connexes

Protocole LACP (Link Aggregation Control Protocol), à la page 641
Personnaliser l'EtherChannel, à la page 648

Personnaliser l'EtherChannel

Cette section décrit comment définir le nombre maximal d'interfaces dans l'EtherChannel, le nombre minimal d'interfaces opérationnelles pour que l'EtherChannel soit actif, l'algorithme d'équilibrage de charges et d'autres paramètres facultatifs.

Procédure

Étape 1 Selon votre mode de contexte :

- Pour le mode unique, choisissez le volet **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.
- Pour le mode multiple dans l'espace d'exécution du système, choisissez le volet **Configuration** > **Context Management (Gestion des contextes)** > **Interfaces**.

Étape 2 Cliquez sur l'interface de canal de port que vous souhaitez personnaliser, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche.

Étape 3 Pour remplacer le type de support, les conditions de duplex, la vitesse et les trames de pause pour le contrôle de flux pour toutes les interfaces membres, cliquez sur **Configure Hardware Properties** (Configurer les propriétés matérielles). Cette méthode offre un raccourci pour définir ces paramètres, car ceux-ci doivent correspondre pour toutes les interfaces du groupe de canaux.

Étape 4 (Facultatif; ISA 3000 uniquement) Pour personnaliser l'EtherChannel, cliquez sur l'onglet **Advanced** (Avancé).

a) Dans la zone **EtherChannel**, dans la liste déroulante **Minimum**, sélectionnez le nombre minimum d'interfaces actives requis pour que l'EtherChannel soit actif, entre 1 et 16. La valeur par défaut est 1.

b) Dans la liste déroulante **Maximum**, choisissez le nombre maximum d'interfaces actives autorisées dans l'EtherChannel, entre 1 et 16. Par défaut, c'est 16. Si votre commutateur ne prend pas en charge 16 interfaces actives, veillez à régler cette commande à 8 ou moins.

c) Dans la liste déroulante **Load Balance** (Équilibrage de charges), sélectionnez les critères utilisés pour équilibrer la charge des paquets sur les interfaces du canal de groupe. Par défaut, l'ASA équilibre la charge de paquets sur les interfaces en fonction de l'adresse IP source et de destination du paquet. Si vous souhaitez modifier les propriétés selon lesquelles le paquet est classé, choisissez un ensemble de critères différent. Par exemple, si votre trafic est fortement orienté vers les mêmes adresses IP de source et de destination, l'affectation du trafic aux interfaces de l'EtherChannel ne sera pas équilibrée. Le passage à un algorithme différent peut entraîner une répartition plus uniforme du trafic. Pour plus d'informations sur l'équilibrage de la charge, consultez Équilibrage de la charge, à la page 642.

d) Pour les paramètres de balisage de groupe sécurisé (**Secure Group Tagging**), consultez le guide de configuration du pare-feu.

e) Pour les paramètres de grappe d'ASA (**ASA Cluster**), consultez (Recommandé; requis en mode de contexte multiple) Configurer les interfaces sur le nœud de contrôle, à la page 387.

Étape 5 Cliquez sur **OK**.

Vous retournez dans le volet **Interfaces**.

Étape 6 Pour définir le mode et la priorité d'une interface physique dans le groupe de canaux :

a) Cliquez sur l'interface physique dans le tableau **Interfaces**, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche.

b) Cliquez sur l'onglet **Advanced (Avancé)**.

c) Dans la zone **EtherChannel**, dans la liste déroulante **Mode**, choisissez **Active** (Actif), **Passive** (Passif) ou **On** (Activé). Nous vous recommandons d'utiliser le mode actif (par défaut).

d) (Facultatif; ISA 3000 uniquement) Dans le champ **LACP Port Priority** (Priorité de port LACP), définissez la priorité de port entre 1 et 65535. La valeur par défaut est 32768. Plus le numéro de priorité est élevé, plus la priorité est faible. L'ASA utilise ce paramètre pour décider quelles interfaces sont actives et lesquelles sont en veille si vous attribuez plus d'interfaces que ce qui peut être utilisé. Si le paramètre de priorité de port est le même pour toutes les interfaces, la priorité est déterminée par l'ID d'interface (logement/port). L'ID d'interface le plus faible correspond à la priorité la plus élevée. Par exemple, GigabitEthernet 0/0 est une priorité plus élevée que GigabitEthernet 0/1.

Si vous souhaitez donner la priorité à une interface pour qu'elle soit active même si elle a un ID d'interface plus élevé, définissez cette commande pour avoir une valeur inférieure. Par exemple, pour activer GigabitEthernet 1/3 avant GigabitEthernet 0/7, faites que la valeur de priorité soit 12345 sur l'interface 1/3 contre la valeur par défaut 32768 sur l'interface 0/7.

Si le périphérique à l'autre extrémité de l'EtherChannel a des priorités de port conflictuelles, la priorité du système est utilisée pour déterminer les priorités de port à utiliser. Consultez l'étape 9 pour définir la priorité de système.

Étape 7 Cliquez sur **OK**.

Vous retournez dans le volet **Interfaces**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Étape 9 (Facultatif; ISA 3000 uniquement) Pour définir la priorité de système LACP, procédez comme suit. Si le périphérique à l'autre extrémité de l'EtherChannel a des priorités de port conflictuelles, la priorité du système est utilisée pour déterminer les priorités de port à utiliser. Consultez l'étape 6d pour obtenir de plus amples renseignements.

a) Selon votre mode de contexte :

- Pour le mode unique, choisissez le volet **Configuration** > **Device Setup (Configuration de l'appareil)** > **EtherChannel**.
- Pour le mode multiple dans l'espace d'exécution du système, choisissez le volet **Configuration** > **Context Management (Gestion des contextes)** > **EtherChannel**.

b) Dans le champ **LACP System Priority** (Priorité de système LACP), saisissez une priorité entre 1 et 65535.

La valeur par défaut est 32768.

Sujets connexes

Équilibrage de la charge, à la page 642
Ajouter des interfaces à l'EthernetChannel, à la page 646

Exemples d'EtherChannels

L'exemple suivant configure trois interfaces dans le cadre d'un EtherChannel. Il définit également la priorité système pour une priorité plus élevée et GigabitEthernet 0/2 pour une priorité plus élevée que les autres interfaces dans le cas où plus de huit interfaces sont affectées à l'EtherChannel.

```
lacp system-priority 1234
interface GigabitEthernet0/0
  channel-group 1 mode active
interface GigabitEthernet0/1
  channel-group 1 mode active
interface GigabitEthernet0/2
  lacp port-priority 1234
  channel-group 1 mode passive
interface Port-channel1
  lacp max-bundle 4
  port-channel min-bundle 2
  port-channel load-balance dst-ip
```

Historique des EtherChannels

Tableau 29 : Historique des EtherChannels

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge EtherChannel	v 8.4(1)	Vous pouvez configurer jusqu'à 48 EtherChannels 802.3ad de huit interfaces actives chacun. Nous avons modifié ou introduit les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Add/Edit EtherChannel Interface (Ajouter/Modifier l'interface EtherChannel) Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier l'interface) Configuration > Device Setup (Configuration de l'appareil) > EtherChannel **Remarque** EtherChannel n'est pas pris en charge sur l'ASA 5505.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de 16 liens actifs dans un EtherChannel	9.2(1)	Vous pouvez maintenant configurer jusqu'à 16 liens actifs dans un EtherChannel. Auparavant, vous pouviez avoir 8 liens actifs et 8 liens de secours. Assurez-vous que votre commutateur peut prendre en charge 16 liens actifs (par exemple, Cisco Nexus 7000 avec module F2-Series 10 Gigabit Ethernet). **Remarque** Si vous effectuez une mise à niveau à partir d'une version antérieure d'ASA, le nombre maximum d'interfaces actives est défini sur 8 à des fins de compatibilité. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit EtherChannel Interface (Ajouter/Modifier l'interface EtherChannel) > Advanced (Avancé).



CHAPITRE 18

Interfaces de boucle avec retour

Ce chapitre explique comment configurer les interfaces de boucle avec retour.

- À propos des interfaces de boucle avec retour, à la page 653
- Directives pour les interfaces de boucle avec retour, à la page 654
- Configurer une interface de boucle avec retour, à la page 654
- Limite de débit du trafic vers l'interface de boucle avec retour, à la page 655
- Historique des interfaces de boucle avec retour, à la page 659

À propos des interfaces de boucle avec retour

Une interface de boucle avec retour est une interface logicielle uniquement qui émule une interface physique. Cette interface est accessible sur IPv4 et IPv6 par l'intermédiaire de plusieurs interfaces physiques. L'interface de boucle avec retour permet de résoudre les échecs de chemin. elle est accessible à partir de n'importe quelle interface physique. Par conséquent, si l'une d'elles tombe en panne, vous pouvez accéder à l'interface de boucle avec retour à partir d'une autre.

Les interfaces de boucle avec retour peuvent être utilisées pour :

- AAA
- BGP
- SNMP
- SSH
- Tunnels VTI statiques et dynamiques
- Syslog
- Telnet

L'ASA peut distribuer l'adresse de boucle avec retour à l'aide de protocoles de routage dynamique, ou vous pouvez configurer une voie de routage statique sur le périphérique homologue pour atteindre l'adresse IP de boucle avec retour par l'une des interfaces physiques de l'ASA. Vous ne pouvez pas configurer une voie de routage statique sur ASA qui spécifie l'interface de boucle avec retour.

Directives pour les interfaces de boucle avec retour

Basculement et mise en grappe

- Aucune prise en charge de mise en grappe.

Mode contextuel

- Le VTI est pris en charge en mode de contexte unique uniquement. Les autres utilisations de la boucle avec retour sont prises en charge en mode contexte multiple.

Directives et limites additionnelles

- La répartition aléatoire des séquences TCP est toujours désactivée pour le trafic de l'interface physique à l'interface de boucle avec retour.

Configurer une interface de boucle avec retour

Ajoutez une interface de boucle avec retour.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.

Étape 2 Choisissez **Add (Ajouter)** > **Loopback Interface (Interface de boucle avec retour)**.

La boîte de dialogue **Add Loopback Interface** (Ajouter une interface de boucle avec retour) s'affiche.

Étape 3 Dans le champ **Loopback ID** (ID de l'interface de boucle avec retour), saisissez un nombre entier entre 0 et 10413.

Étape 4 Si l'interface n'est pas déjà activée, cochez la case **Enable Interface** (Activer l'interface).

L'interface est activée par défaut.

Étape 5 (Facultatif) Saisissez une description dans le champ **Description**.

Étape 6 Configurez le nom et l'adresse IP. Consultez Interfaces en mode routage et en mode transparent, à la page 693

Étape 7 Cliquez sur **OK**.

Vous retournez dans le volet **Interfaces**.

Étape 8 Configurez la limitation de débit pour le trafic de boucle avec retour. Consultez Limite de débit du trafic vers l'interface de boucle avec retour, à la page 655.

Limite de débit du trafic vers l'interface de boucle avec retour

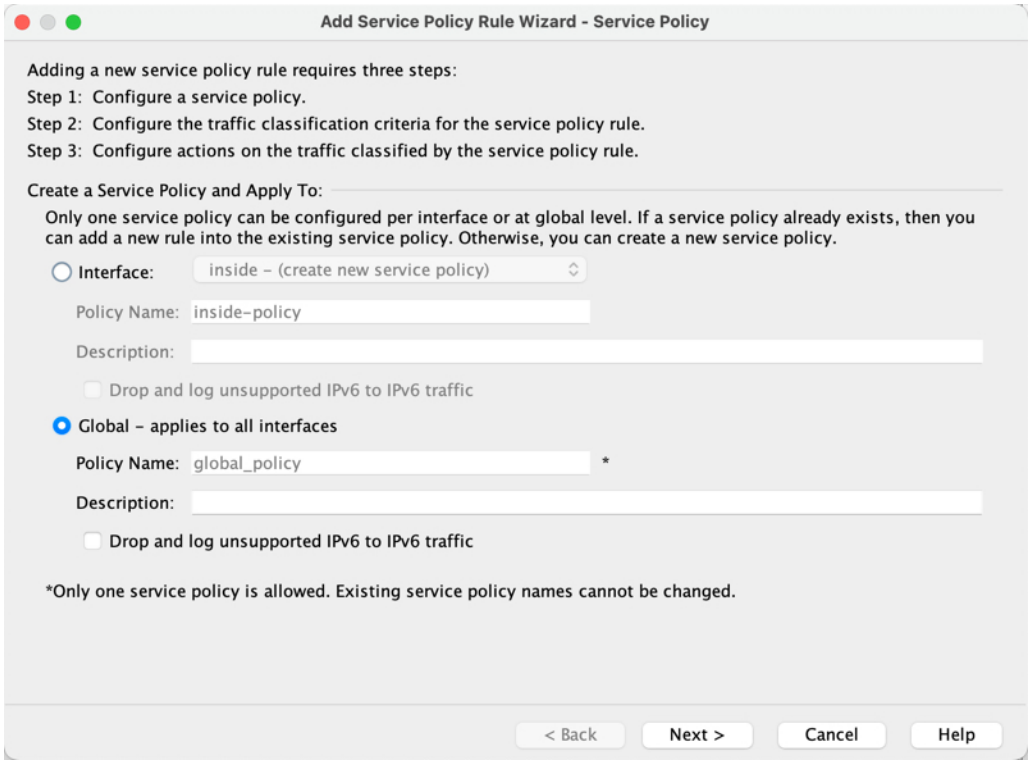
Vous devez limiter le trafic vers l'adresse IP de l'interface de boucle avec retour pour éviter une charge excessive sur le système. Vous pouvez ajouter une règle de limite de connexion à la politique de service globale. Cette procédure montre l'ajout à la politique globale par défaut (global_policy).

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Service Policy (Politique de service)**, puis cliquez sur **Add (Ajouter)** > **Add Service Policy Rule (Ajouter une règle de politique de service)**.

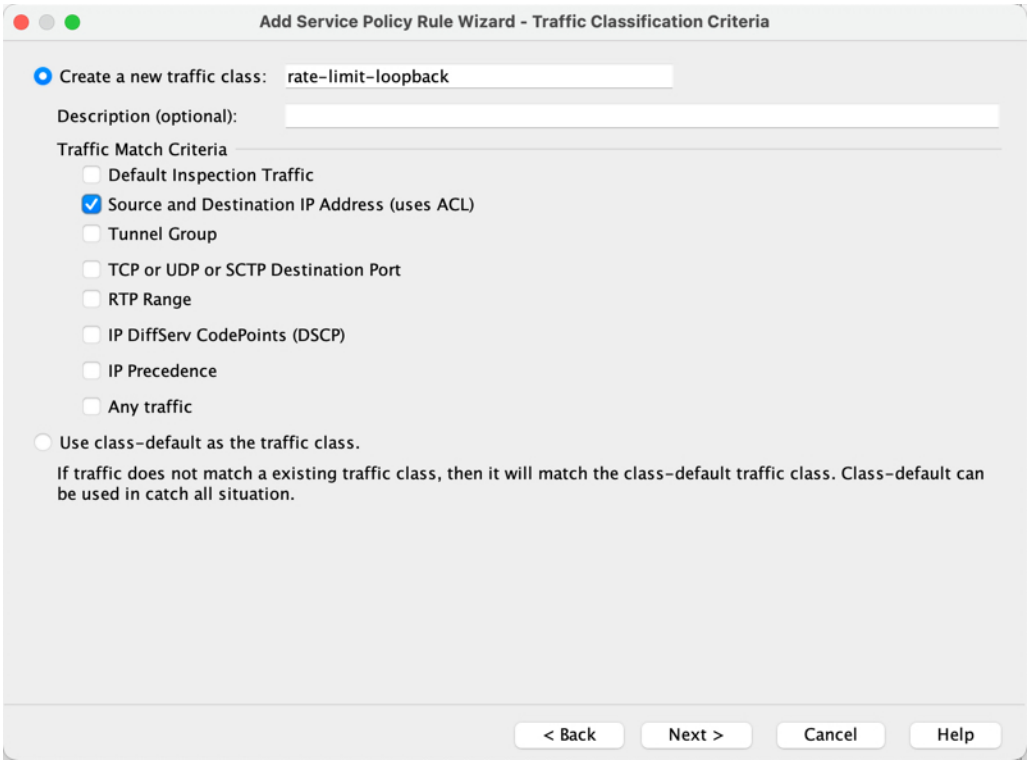
Étape 2 Sélectionnez la politique **Global** (Globale) et cliquez sur **Next** (Suivant).

Illustration 72 : Politique de service



Étape 3 Sur la page **Traffic Classification Criteria** (Critères de classification du trafic), définissez les valeurs suivantes et cliquez sur **Next** (Suivant).

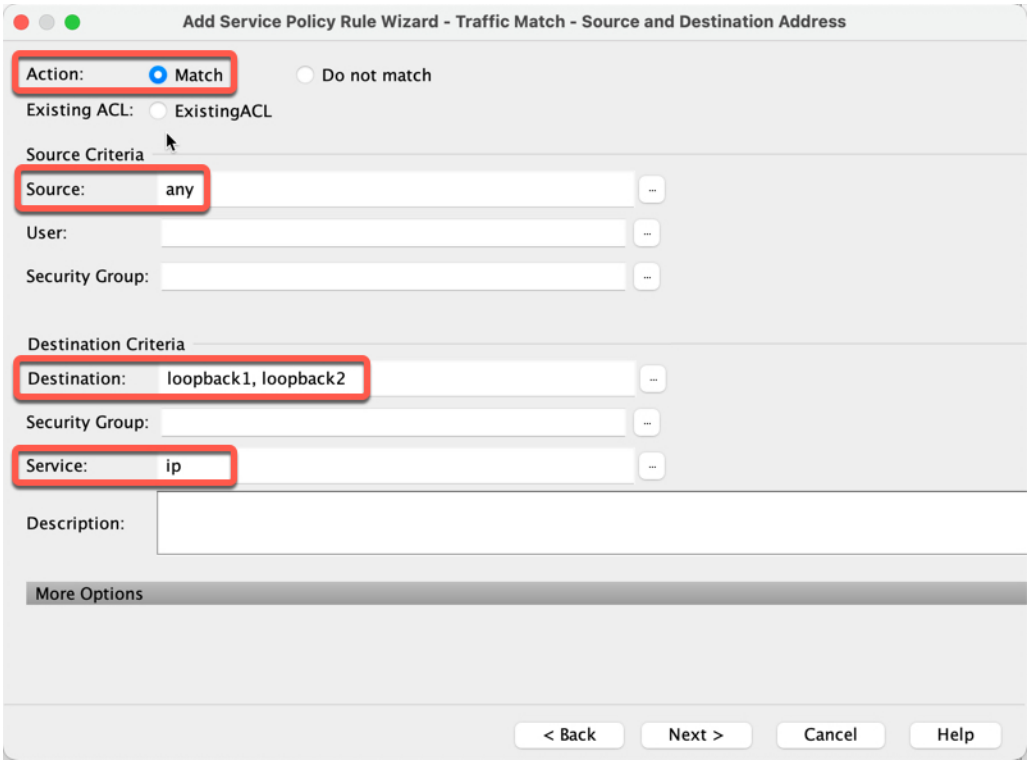
Illustration 73 : Critères de classification du trafic



- **Create a new traffic class** (Créer une nouvelle classe de trafic) : nommez la classe de trafic de boucle avec retour.
- **Source and Destination IP Address (uses ACL)** (Adresse IP source et de destination (utilise ACL))

Étape 4 Sur la page **Traffic Match - Source and Destination Address** (Concordance de trafic – Adresse source et de destination), définissez la liste de contrôle d'accès pour spécifier tout le trafic IP allant à l'adresse IP de boucle avec retour, puis cliquez sur **Next** (Suivant).

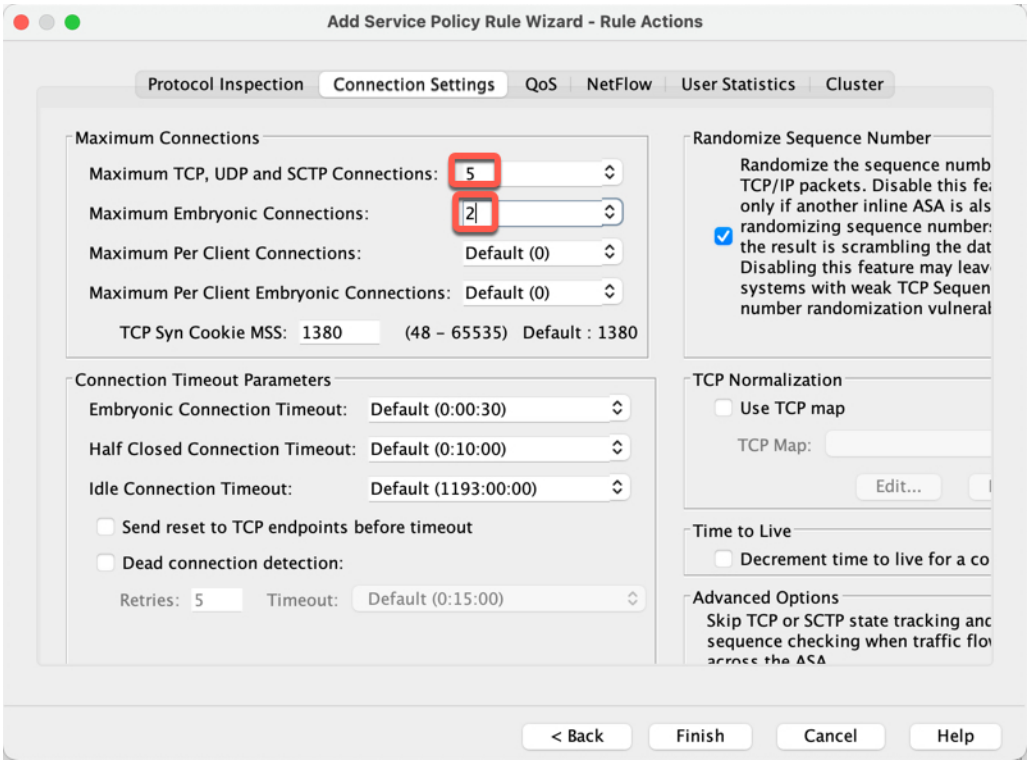
Illustration 74 : Correspondance de trafic – Adresse source et de destination



- **Action: Match** (Action : Mettre en correspondance)
- **Source** : toute. Vous pouvez également restreindre cette liste d'accès en spécifiant les adresses IP source plutôt que **any** (toute).
- **Destination** : les adresses IP de l'interface de boucle avec retour
- **Service** : ip

Étape 5 Sur la page **Rule Actions** (Actions découlant d'une règle), cliquez sur l'onglet **Connection Settings** (Paramètres de connexion) et dans la zone **Maximum Connections** (Nombre maximum de connexions), définissez les valeurs suivantes.

Illustration 75 : Actions découlant d'une règle

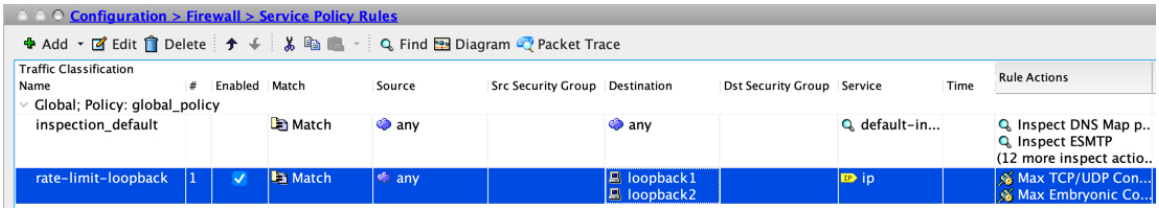


- **Maximum TCP, UDP and SCTP Connections** (Nombre maximum de connexions TCP, UDP et SCTP) : définissez le nombre maximum de connexions TCP et UDP sur le nombre attendu de connexions pour l'interface de boucle avec retour et le nombre de connexions amorces à un nombre inférieur. Par exemple, vous pouvez lui attribuer la valeur **5/2**, **10/5** ou **1024/512**, selon le nombre de sessions d'interface de boucle avec retour attendues dont vous avez besoin.
- **Embryonic Connections** (Connexions amorces) : la définition de la limite de connexions amorces active l'interception de TCP, qui protège le système contre une attaque DoS perpétrée en inondant une interface de paquets SYN de TCP.

Étape 6 Cliquez sur **Finish** (Terminer).

La règle est ajoutée à la politique globale.

Illustration 76 : Tableau des règles de politique de service



Étape 7 Cliquez sur **Apply** (Appliquer).

Historique des interfaces de boucle avec retour

Tableau 30 : Historique des interfaces de boucle avec retour

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge de l'interface de boucle avec retour pour VTI	9.19(1)	Une interface de boucle avec retour fournit la redondance des tunnels VPN VTI statiques et dynamiques. Vous pouvez désormais définir une interface de bouclage comme interface source pour un VTI. L'interface VTI peut également hériter de l'adresse IP d'une interface de boucle avec retour au lieu d'une adresse IP configurée de manière statique. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP de l'interface de boucle avec retour. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add VTI Interface (ajouter une interface VTI)** > **Advanced (avancé)**.
Prise en charge par ASDM des interfaces de bouclage	9.19(1)	ASDM prend désormais en charge les interfaces de bouclage. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add Loopback Interface (ajouter une interface de bouclage)**.
Prise en charge de l'interface de boucle avec retour	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour : • BGP • AAA • SNMP • Journal système • SSH • Telnet Commandes nouvelles ou modifiées : **interface loopback**, **logging host**, **neighbor update-source**, **snmp-server host**, **ssh**, **telnet** ASDM n'est pas pris en charge.



CHAPITRE 19

Sous-interfaces VLAN

Ce chapitre explique comment configurer les sous-interfaces VLAN.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà dans l'espace d'exécution du système, dans le volet Configuration > Device List (Liste des périphériques), double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

- À propos des sous-interfaces VLAN, à la page 661
- Licences pour les sous-interfaces VLAN, à la page 661
- Lignes directrices et limites pour les sous-interfaces VLAN, à la page 662
- Paramètres par défaut pour les sous-interfaces VLAN, à la page 663
- Configurer les sous-interfaces VLAN et la jonction 802.1Q, à la page 663
- Exemples de sous-interfaces VLAN, à la page 665
- Historique des sous-interfaces VLAN, à la page 666

À propos des sous-interfaces VLAN

Les sous-interfaces VLAN vous permettent de diviser une interface physiqueou EtherChannel en plusieurs interfaces logiques qui sont étiquetées avec différents ID de VLAN. Une interface avec une ou plusieurs sous-interfaces VLAN est automatiquement configurée comme une ligne principale 802.1Q. Comme les réseaux VLAN vous permettent de garder le trafic séparé sur une interface physique donnée, vous pouvez augmenter le nombre d'interfaces disponibles pour votre réseau sans ajouter d'interfaces physiques ou d'ASA supplémentaires. Cette fonctionnalité est particulièrement utile en mode de contexte multiple, car vous pouvez affecter des interfaces uniques à chaque contexte.

Vous pouvez configurer un VLAN principal ainsi qu'un ou plusieurs VLAN secondaires. Lorsque l'ASA reçoit le trafic sur les VLAN secondaires, il le mappe au VLAN principal.

Licences pour les sous-interfaces VLAN

Modèle	Exigence de licence
Firepower 1010	Licence Essentials : 60

Modèle	Exigence de licence
Firepower 1120	Licence Essentials : 512
Firepower 1140, 1150	Licence Essentials : 1 024
Firepower de la série 2100	Licence Essentials : 1 024
Secure Firewall 3100	Licence Essentials : 1 024
Firepower 4100	Licence Essentials : 1 024
Firepower 9300	Licence Essentials : 1 024
ASA virtuel	Capacité de débit : 100 Mbit/s : 25 1 Gbit/s : 50 2 Gbit/s : 200 10 Gbit/s : 1 024
ISA 3000	LicenceEssentials : 5 Licence Security Plus : 100

Remarque Pour qu'une interface soit prise en compte dans la limite de VLAN, vous devez lui attribuer un VLAN.

Lignes directrices et limites pour les sous-interfaces VLAN

Prise en charge des modèles

- 1010 —Les sous-interfaces ne sont pas prises en charge sur les ports de commutation ou les interfaces VLAN.
- Pour les modèles ASA, vous ne pouvez pas configurer de sous-interface sur l'interface de gestion. Consultez L'interface de logement/port de gestion, à la page 612 pour la prise en charge des sous-interfaces.

Directives supplémentaires

- Prévention des paquets non balisés sur l'interface physique : Si vous utilisez des sous-interfaces, vous ne souhaitez généralement pas que l'interface physique achemine le trafic, car l'interface physique peut transmettre des paquets non balisés. Cette propriété est également vraie pour l'interface physique active pour les liaisons EtherChannel. Étant donné que l'interface physique ou EtherChannel doit être activée pour que la sous-interface achemine le trafic, assurez-vous que l'interface physique ou EtherChannel ne transmet pas le trafic en ne configurant pas de nom pour l'interface. Si vous voulez laisser l'interface

physique ou EtherChannel passer des paquets non balisés, vous pouvez configurer la commande name comme d'habitude.

- Toutes les sous-interfaces de la même interface parente doivent soit être des membres de groupes de ponts, soit des interfaces routées; vous ne pouvez pas combiner les deux types.
- L'ASA ne prend pas en charge le protocole DTP (Dynamic Trunking Protocol), vous devez donc configurer le port de commutation connectée pour qu'il assure la liaison sans condition.
- Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur l'ASA, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur ASA. Vous pouvez générer automatiquement des adresses MAC uniques; voir Attribuer automatiquement des adresses MAC, à la page 736.

Remarque Si vous attribuez manuellement une adresse MAC, veillez à attribuer des adresses MAC à toutes les sous-interfaces sur la même interface physique pour éviter les comportements imprévus et les pannes.

Paramètres par défaut pour les sous-interfaces VLAN

Cette section répertorie les paramètres par défaut des interfaces si vous n'avez pas de configuration d'usine par défaut.

État par défaut des interfaces

L'état par défaut d'une interface dépend du type d'interface et du mode de contexte.

En mode de contexte multiple, toutes les interfaces allouées sont activées par défaut, quel que soit l'état de l'interface dans l'espace d'exécution du système. Cependant, pour que le trafic passe par l'interface, celle-ci doit également être activée dans l'espace d'exécution du système. Si vous désactivez une interface dans l'espace d'exécution du système, cette interface est désactivée dans tous les contextes qui la partagent.

En mode unique ou dans l'espace d'exécution du système, les interfaces ont les états par défaut suivants :

- Interfaces physiques : désactivées.
- Sous-interfaces VLAN : activées. Cependant, pour que le trafic passe par la sous-interface, l'interface physique doit également être activée.

Configurer les sous-interfaces VLAN et la jonction 802.1Q

Ajoutez une sous-interface VLAN à une interface physique ou EtherChannel.

Avant de commencer

Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système.. Si vous n'êtes pas déjà en mode de configuration système, dans le volet **Configuration > Device List (Liste des périphériques)**, double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Selon votre mode de contexte :

- Pour le mode unique, choisissez le volet **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces**.
- Pour le mode multiple dans l'espace d'exécution du système, choisissez le volet **Configuration > Context Management (Gestion des contextes) > Interfaces** .

Étape 2 Choisissez **Add (Ajouter)** > **Interface**.

La boîte de dialogue **Add Interface** (Ajouter une interface) apparaît.

Remarque En mode unique, cette procédure ne couvre qu'un sous-ensemble des paramètres de la boîte de dialogue Edit Interface (Modifier l'interface); pour configurer d'autres paramètres, consultez Interfaces en mode routage et en mode transparent, à la page 693. Notez qu'en mode de contexte multiple, avant de terminer la configuration de l'interface, vous devez attribuer des interfaces aux contextes. Consultez Configurer plusieurs contextes, à la page 269.

Étape 3 Dans la liste déroulante **Hardware Port** (Port matériel), choisissez l'interface physique ou de canal de port à laquelle vous souhaitez ajouter la sous-interface.

Étape 4 Si l'interface n'est pas déjà activée, cochez la case **Enable Interface** (Activer l'interface).

L'interface est activée par défaut.

Étape 5 Dans le champ **VLAN ID** (ID VLAN), entrez un numéro VLAN compris entre 1 et 4 094.

Certains numéros de VLAN peuvent être réservés sur les commutateurs connectés. Consultez la documentation du commutateur pour en savoir plus. Pour le mode de contexte multiple, vous pouvez uniquement définir le VLAN dans la configuration système.

Étape 6 Dans le champ **Secondary VLAN ID** (ID de VLAN secondaire), saisissez un ou plusieurs ID de VLAN, séparés par des espaces, des virgules ou des tirets (pour une plage contiguë).

Lorsque l'ASA reçoit le trafic sur les VLAN secondaires, il mappe le trafic au VLAN principal.

Étape 7 Dans le champ **Subinterface ID** (ID de sous-interface), saisissez l'ID de la sous-interface sous la forme d'un nombre entier compris entre 1 et 4294967293.

Le nombre de sous-interfaces autorisés dépend de votre plateforme. Vous ne pouvez pas modifier l'ID après l'avoir défini.

Étape 8 (Facultatif) Dans le champ **Description**, saisissez une description pour cette interface.

La description peut contenir jusqu'à 240 caractères sur une seule ligne (sans retour chariot). Pour le mode de contexte multiple, la description du système est indépendante de la description du contexte. Dans le cas d'une liaison de basculement ou d'état, la description fixe est « LAN Failover Interface », « STATE Failover Interface » ou « LAN/STATE Failover Interface » par exemple. Vous ne pouvez pas modifier cette description. La description fixe remplace toute description que vous saisissez ici si vous faites de cette interface une liaison de basculement ou un lien d'état.

Étape 9 Cliquez sur **OK**.

Vous retournez dans le volet **Interfaces**.

Sujets connexes

Licences pour les sous-interfaces VLAN, à la page 661

Exemples de sous-interfaces VLAN

L'exemple suivant configure les paramètres d'une sous-interface en mode unique :

```
interface gigabitethernet 0/1
  no nameif
  no security-level
  no ip address
  no shutdown
interface gigabitethernet 0/1.1
  vlan 101
  nameif inside
  security-level 100
  ip address 192.168.6.6 255.255.255.0
  no shutdown
```

L'exemple suivant montre comment le mappage de VLAN fonctionne avec le commutateur Catalyst 6500. Consultez le guide de configuration du commutateur Catalyst 6500 pour savoir comment connecter des nœuds à des PVLAN.

ASA Configuration

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

```
Catalyst 6500 Configuration

vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

Historique des sous-interfaces VLAN

Tableau 31 : Historique des sous-interfaces VLAN

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Augmentation du nombre de VLAN	7.0(5)	Augmentation des limites suivantes : • VLAN de licences de base ASA 5510 de 0 à 10. • VLAN de licences Security Plus ASA 5510, 10 à 25. • VLAN ASA 5520 de 25 à 100. • VLAN ASA 5540 de 100 à 200.
Augmentation du nombre de VLAN	7.2(2)	Les limites de VLAN ont été augmentées pour l'ASA 5510 (de 10 à 50 pour la licence de base et de 25 à 100 pour la licence Security Plus), l'ASA 5520 (de 100 à 150), l'ASA 5550 (de 200 à 250).
Augmentation du nombre de VLAN pour l'ASA 5580	8.1(2)	Le nombre de VLAN pris en charge sur l'ASA 5580 est passé de 100 à 250.
Prise en charge du mappage d'un VLAN secondaire à un VLAN principal	9.5(2)	Vous pouvez maintenant configurer un ou plusieurs VLAN secondaires pour une sous-interface. Lorsque l'ASA reçoit le trafic sur les VLAN secondaires, il le mappe au VLAN principal. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add Interface (Ajouter une interface)** > **General (Général)**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Augmentation du nombre de VLAN pour l'ISA 3000	9.13(1)	Le nombre maximum de VLAN pour l'ISA 3000 avec la licence Security Plus est passé de 25 à 100.



CHAPITRE 20

Interfaces VXLAN

Ce chapitre explique comment configurer des interfaces Virtual eXtensible LAN (VXLAN). Les VXLAN agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3 pour étendre les réseaux de couche 2.

- À propos des interfaces VXLAN, à la page 669
- Exigences et conditions préalables pour les interfaces VXLAN, à la page 679
- Lignes directrices pour les interfaces VXLAN, à la page 680
- Paramètres par défaut des interfaces VXLAN, à la page 681
- Configurer les interfaces VXLAN, à la page 681
- Configurer les interfaces Geneve, à la page 683
- Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle, à la page 685
- Exemples d'interfaces VXLAN, à la page 686
- Historique des interfaces VXLAN, à la page 690

À propos des interfaces VXLAN

Le réseau VXLAN fournit les mêmes services de réseau Ethernet de couche 2 que le réseau VLAN, mais avec une extensibilité et une flexibilité accrues. Par rapport au VLAN, le VXLAN offre les avantages suivants :

- Emplacement flexible des segments multidétenteurs dans le centre de données.
- Évolutivité accrue pour traiter un plus grand nombre de segments de couche 2 : jusqu'à 16 millions de segments VXLAN.

Cette section décrit le fonctionnement de VXLAN. Pour en savoir plus sur VXLAN, consultez RFC 7348. Pour des informations détaillées sur Geneve, consultez RFC 8926.

Encapsulation

L'ASA prend en charge deux types d'encapsulation VXLAN :

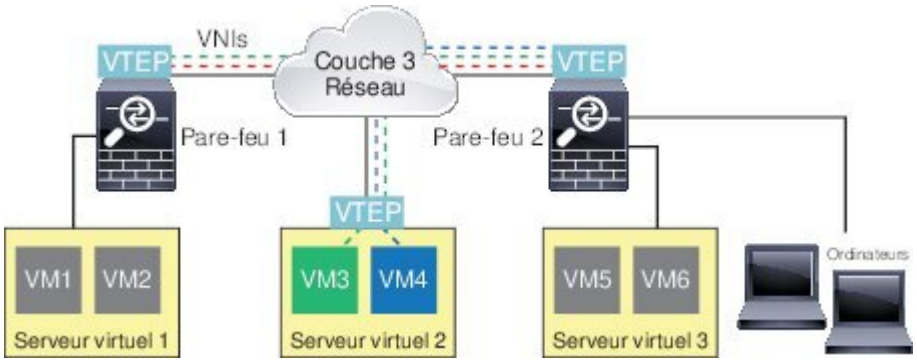
- VXLAN (tous les modèles) : VXLAN utilise l'encapsulation MAC Address-in-User Datagram Protocol (MAC-in-UDP). Un en-tête VXLAN est ajouté à la trame de couche 2 d'origine, qui est ensuite placée dans un paquet UDP-IP.
- Geneve (ASA virtuel uniquement) : Geneve a un en-tête interne flexible qui ne se limite pas à l'adresse MAC. L'encapsulation Geneve est requise pour un routage transparent des paquets entre un équilibreur

de charge de passerelle Amazon Web Services (AWS) et les périphériques, et pour l'envoi d'informations supplémentaires.

Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP a deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier) auxquelles vous appliquez votre politique de sécurité, et une interface normale appelée l'interface source VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

La figure suivante montre deux ASA et le serveur virtuel 2 agissant comme des VTEP dans un réseau de couche 3 et étendant les réseaux VNI 1, 2 et 3 entre les sites. Les ASA agissent comme des ponts ou des passerelles entre les réseaux VXLAN et les non-VXLAN.



Le réseau IP sous-jacent entre les VTEP est indépendant de la superposition VXLAN. Les paquets encapsulés sont acheminés en fonction de l'en-tête d'adresse IP externe, qui a le VTEP de départ comme adresse IP source et le VTEP de fin comme adresse IP de destination. Pour l'encapsulation VXLAN : l'adresse IP de destination peut être un groupe de multidiffusion lorsque le VTEP distant est inconnu. Avec Geneve, l'ASA ne prend en charge que les homologues statiques. Le port de destination de VXLAN est le port UDP 4789 par défaut (configurable par l'utilisateur). Le port de destination pour Geneve est le 6081.

Interface de la source VTEP

L'interface source de VTEP est une interface ASA normale (physique, EtherChannel ou même VLAN) à laquelle vous prévoyez d'associer toutes les interfaces VNI. Vous pouvez configurer une interface source de VTEP par ASA ou contexte de sécurité. Comme vous ne pouvez configurer qu'une seule interface source de VTEP, vous ne pouvez pas configurer les deux interfaces VXLAN et Geneve sur le même périphérique.Il y a une exception pour la mise en grappe d'ASA virtuel sur AWS, où vous pouvez avoir deux interfaces sources VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe, et une interface Geneve peut être utilisée pour l'équilibreur de charges de la passerelle.

L'interface source de VTEP peut être entièrement dédiée au trafic VXLAN, bien qu'elle ne se limite pas à cet usage. Si vous le souhaitez, vous pouvez utiliser l'interface pour le trafic normal et appliquer une politique de sécurité à l'interface pour ce trafic. Pour le trafic VXLAN, cependant, toute la politique de sécurité doit être appliquée aux interfaces VNI. L'interface VTEP sert uniquement de port physique.

En mode de pare-feu transparent, l'interface source de VTEP ne fait pas partie d'un BVI, et vous configurez une adresse IP pour elle, similaire à la façon dont l'interface de gestion est traitée.

Interface VNIs

Les interfaces VNI sont similaires aux interfaces VLAN : ce sont des interfaces virtuelles qui séparent le trafic réseau sur une interface physique donnée en utilisant le balisage. Vous appliquez votre politique de sécurité directement à chaque interface VNI.

Vous ne pouvez ajouter qu'une seule interface VTEP et toutes les interfaces VNI sont associées à la même interface VTEP.Il existe une exception pour la mise en grappe d'ASA virtuel sur AWS. Pour la mise en grappe d'AWS, vous pouvez avoir deux interfaces source VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe et une interface Geneve peut être utilisée pour AWS Gateway Load Balancer.

Traitement de paquet VXLAN

VXLAN

Le trafic entrant et sortant de l'interface source du VTEP est soumis au traitement VXLAN, en particulier à l'encapsulation ou à la désencapsulation.

Le traitement d'encapsulation comprend les tâches suivantes :

- L'interface source du VTEP encapsule la trame MAC interne avec l'en-tête VXLAN.
- Le champ de la somme de contrôle UDP est mis à zéro.
- L'adresse IP de la source de trame externe est définie sur l'adresse IP de l'interface VTEP.
- L'adresse IP de destination de la trame externe est déterminée par une recherche IP distante du VTEP.

Désencapsulation : l'ASA désencapsule un paquet VXLAN uniquement dans les cas suivants :

- Il s'agit d'un paquet UDP dont le port de destination est 4789 (cette valeur peut être configurée par l'utilisateur).
- L'interface d'entrée est l'interface source du VTEP.
- L'adresse IP de l'interface d'entrée est la même que l'adresse IP de destination.
- Le format des paquets VXLAN est conforme à la norme.

Geneve

Le trafic entrant et sortant de l'interface source du VTEP est soumis au traitement de Geneve, en particulier à l'encapsulation ou à la désencapsulation.

Le traitement d'encapsulation comprend les tâches suivantes :

- L'interface source du VTEP encapsule la trame MAC interne avec l'en-tête Geneve.
- Le champ de la somme de contrôle UDP est mis à zéro.
- L'adresse IP de la source de trame externe est définie sur l'adresse IP de l'interface VTEP.
- L'adresse IP de destination de la trame externe est définie sur l'adresse IP homologue que vous avez configurée.

Désencapsulation : l'ASA désencapsule un paquet Geneve uniquement dans les cas suivants :

- Il s’agit d’un paquet UDP dont le port de destination est 6081 (cette valeur peut être configurée par l’utilisateur).
- L’interface d’entrée est l’interface source du VTEP.
- L’adresse IP de l’interface d’entrée est la même que l’adresse IP de destination.
- Le format des paquets Geneve est conforme à la norme.

Pair VTEP

Lorsque l’ASA envoie un paquet à un périphérique derrière un VTEP homologue, l’ASA a besoin de deux renseignements importants :

- L’adresse MAC de destination du périphérique distant
- L’adresse IP de destination du VTEP homologue

L’ASA gère un mappage des adresses MAC de destination sur les adresses IP du VTEP distant pour les interfaces VNI.

Homologue VXLAN

L’ASA peut trouver ces renseignements de deux manières :

- Une adresse IP VTEP homologue unique peut être configurée de manière statique sur l’ASA.

  Vous ne pouvez pas définir manuellement plusieurs homologues.

  L’ASA envoie ensuite une diffusion ARP encapsulée dans VXLAN au VTEP pour connaître l’adresse MAC du nœud d’extrémité.

- Un groupe de multidiffusion peut être configuré sur chaque interface VNI (ou sur le VTEP dans son ensemble).

Remarque Cette option n’est pas prise en charge par Geneve.

: l’ASA envoie un paquet de diffusion ARP encapsulé dans VXLAN dans un paquet IP de multidiffusion par l’intermédiaire de l’interface source de VTEP. La réponse à cette requête ARP permet à l’ASA d’apprendre à la fois l’adresse IP du VTEP distant ainsi que l’adresse MAC de destination du nœud d’extrémité distant.

Homologue Geneve

L’ASA virtuel ne prend en charge que les homologues définis de manière statique. Vous pouvez définir l’adresse IP homologue ASA virtuel sur l'équilibreur de charge de passerelle AWS. Comme l’ASA virtuel n’initie jamais le trafic vers l’équilibreur de charges de passerelle, vous n’avez pas besoin de préciser l’adresse IP de l’équilibreur de charges de passerelle sur l’ASA virtuel; il connaît l’adresse IP homologue lorsqu’il reçoit le trafic de Geneve. Les groupes de multidiffusion ne sont pas pris en charge avec Geneve.

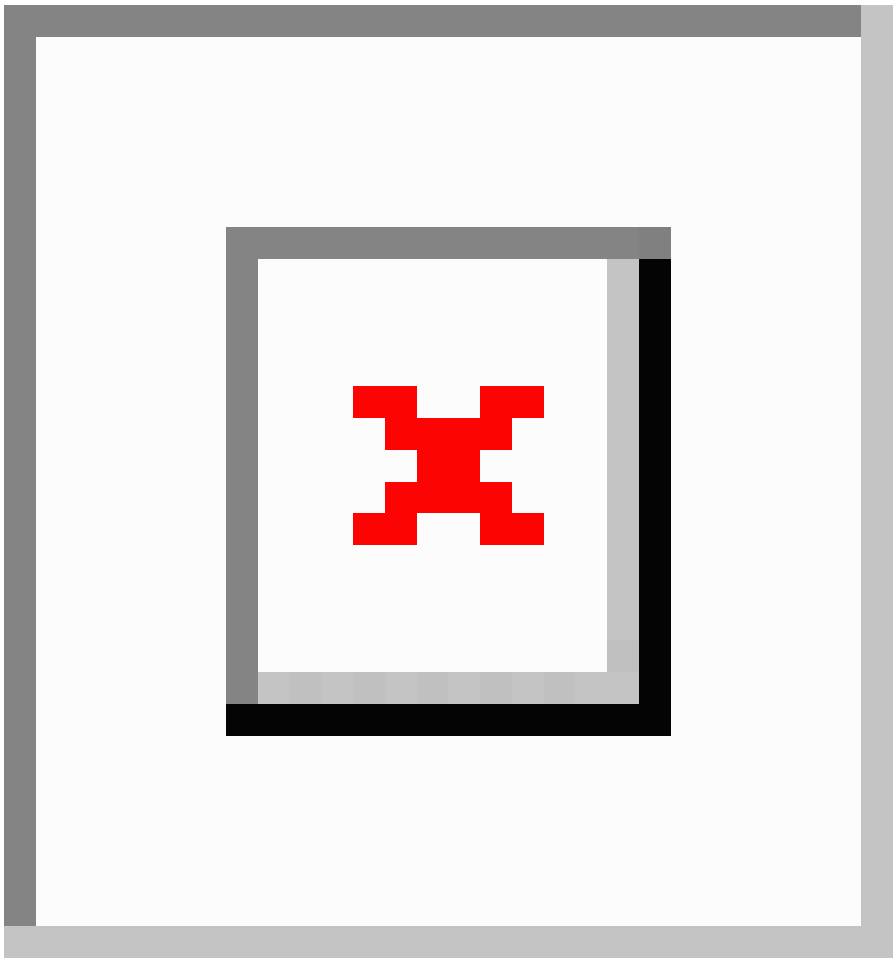
Scénarios VXLAN

Cette section décrit les scénarios d'utilisation de la mise en œuvre de VXLAN sur l'ASA.

Présentation du pont ou de la passerelle VXLAN

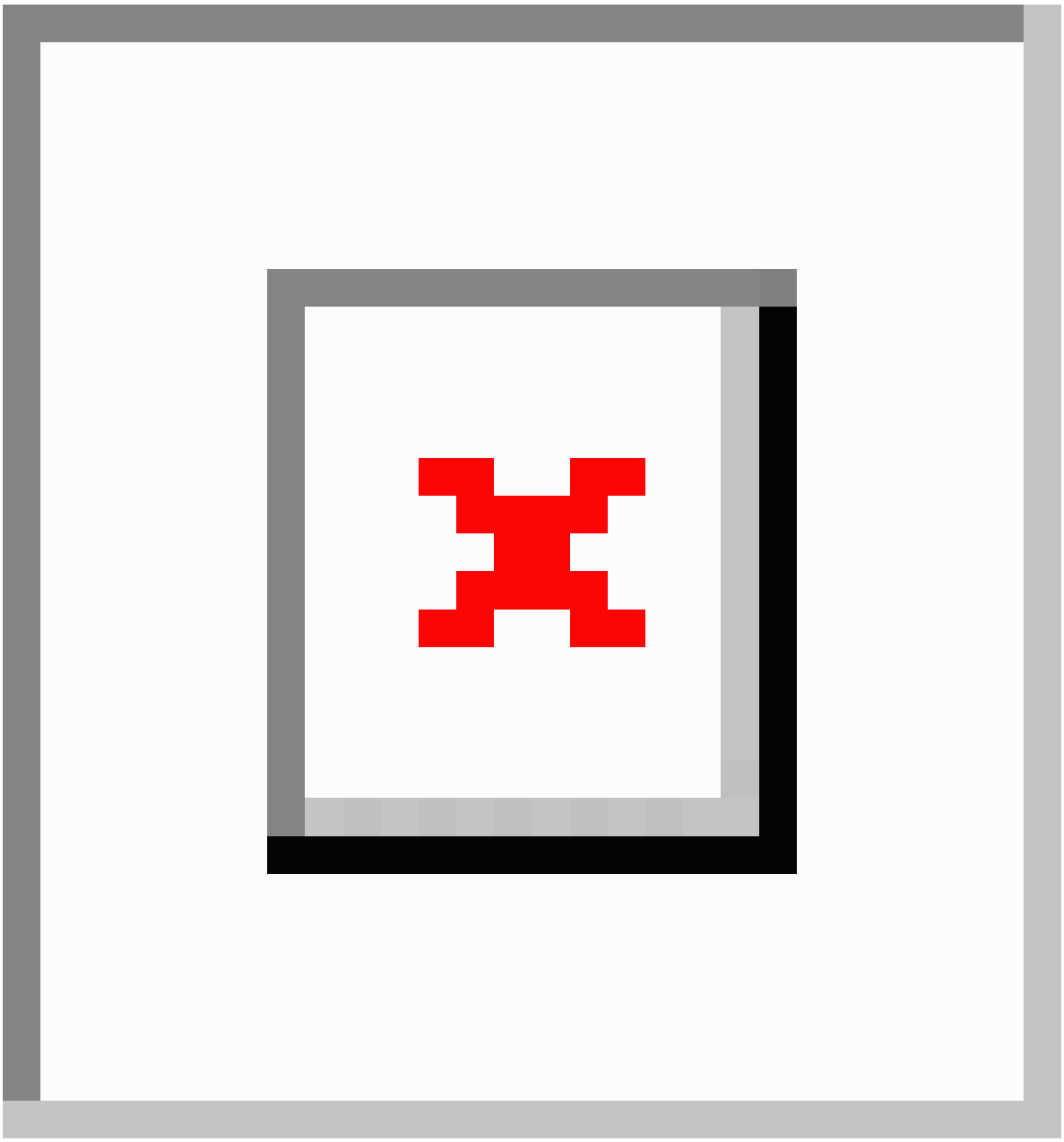
Chaque VTEP ASA agit comme un pont ou une passerelle entre les nœuds terminaux comme les machines virtuelles, les serveurs et les PC et le réseau de superposition VXLAN. Pour les trames entrantes reçues avec encapsulation VXLAN sur l'interface source de VTEP, ASA supprime l'en-tête VXLAN et le transfère vers une interface physique connectée à un réseau non VXLAN en fonction de l'adresse MAC de destination de la trame Ethernet interne.

L'ASA traite toujours les paquets VXLAN; il ne se contente pas de transférer des paquets VXLAN inchangés entre deux autres VTEP.



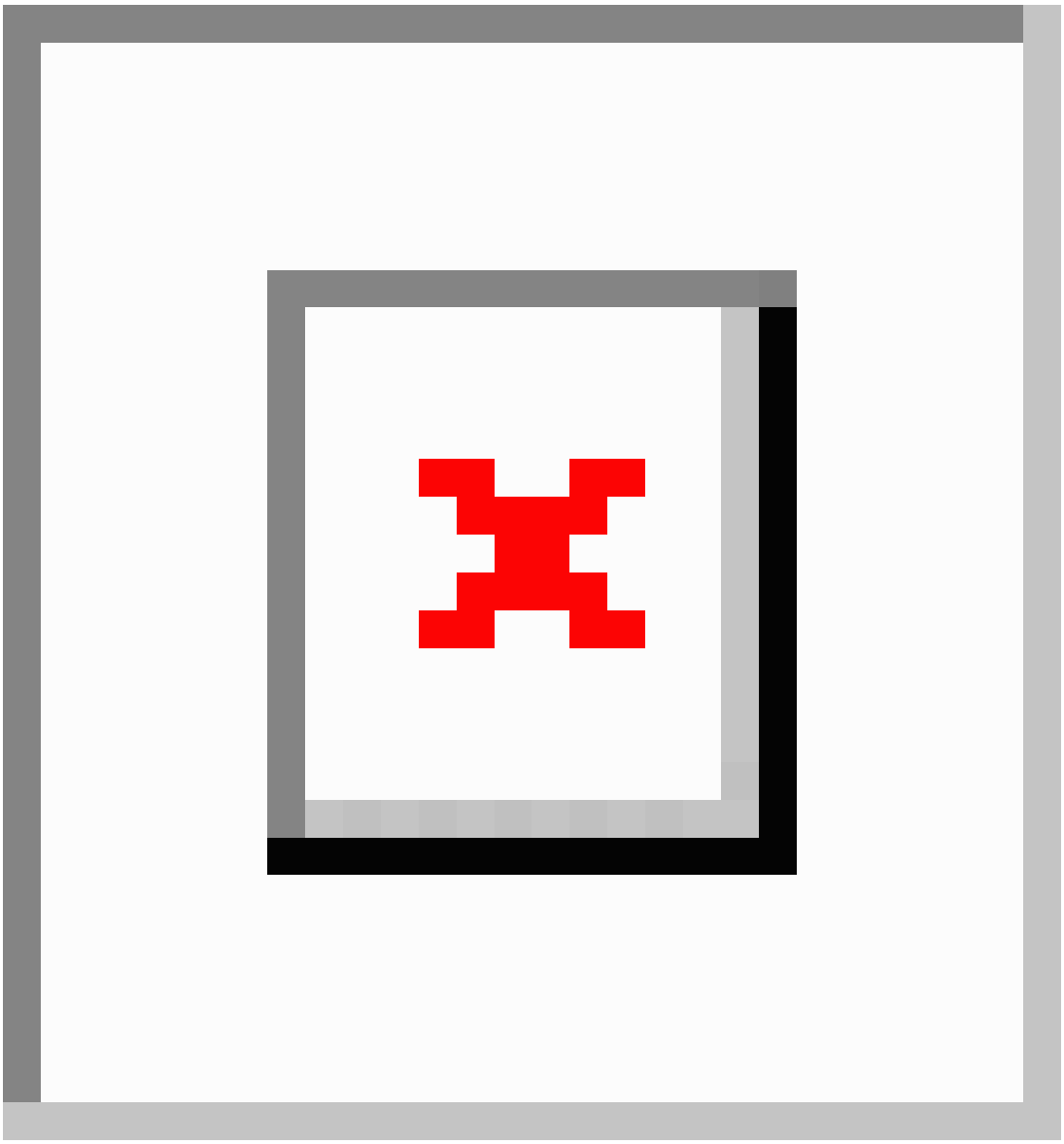
Pont VXLAN

Lorsque vous utilisez un groupe de ponts (mode de pare-feu transparent ou mode de routage facultatif), ASA peut servir de pont VXLAN entre un segment VXLAN (distant) et un segment local, où les deux se trouvent dans le même réseau. Dans ce cas, un membre du groupe de ponts est une interface standard tandis que l'autre membre est une interface VNI.



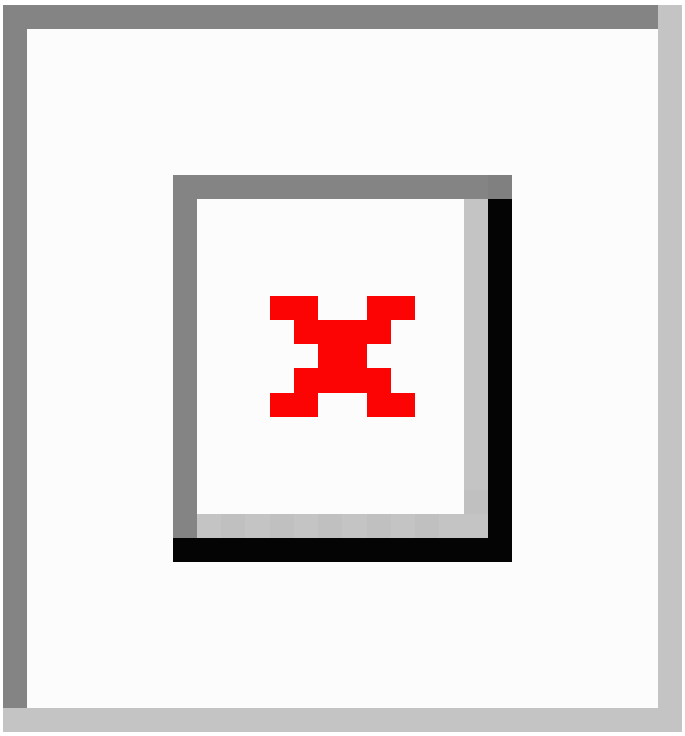
Passerelle VXLAN (mode routé)

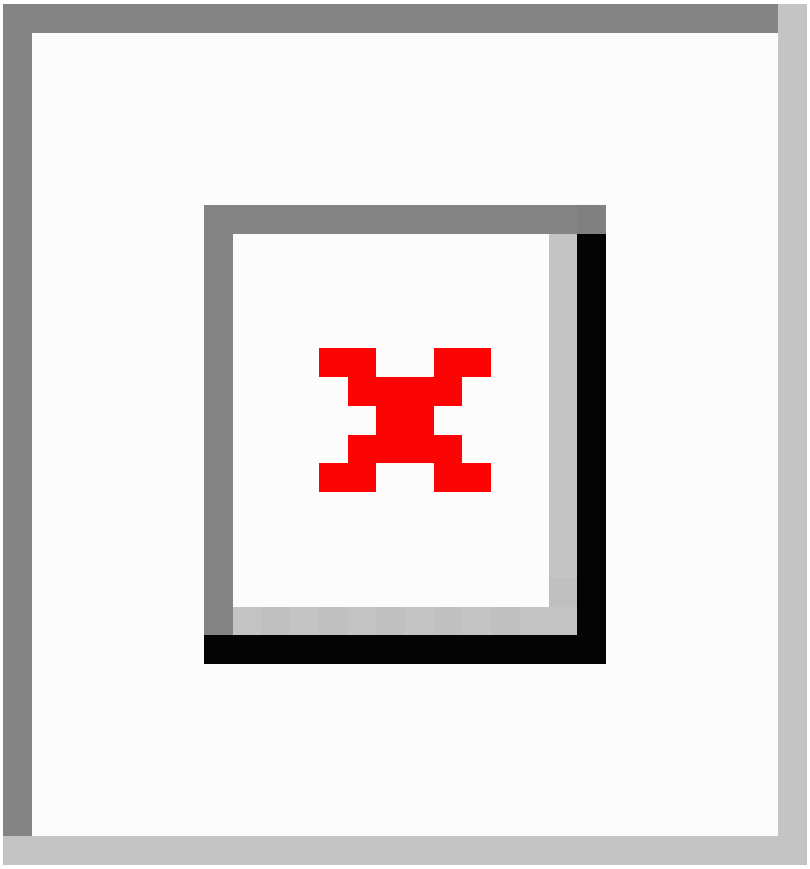
L'ASA peut servir de routeur entre les domaines VXLAN et non-VXLAN, connectant des périphériques sur différents réseaux.



Routeur entre domaines VXLAN

Avec un domaine de couche 2 étendu par VXLAN, une machine virtuelle peut pointer vers un ASA comme passerelle lorsque ASA ne se trouve pas sur le même rack, ou même lorsque l'ASA est éloigné sur le réseau de couche 3.





Consultez les remarques suivantes à propos de ce scénario :

1. Pour les paquets de la VM3 à la VM1, l'adresse MAC de destination est l'adresse MAC ASA, car l'ASA est la passerelle par défaut.
2. L'interface source de VTEP sur le serveur virtuel 2 reçoit les paquets de VM3, puis encapsule les paquets avec la balise VXLAN de VNI 3 et les envoie à l'ASA.
3. Lorsque l'ASA reçoit les paquets, il désencapsule les paquets pour obtenir les trames internes.
4. L'ASA utilise les cadres internes pour la recherche de routage, puis trouve que la destination est sur VNI 2. S'il n'a pas encore de mappage pour VM1, l'ASA envoie une diffusion ARP encapsulée sur l'adresse IP du groupe de multidiffusion sur VNI 2.

Remarque L'ASA doit utiliser la découverte d'homologues VTEP dynamique, car il a plusieurs homologues VTEP dans ce scénario.

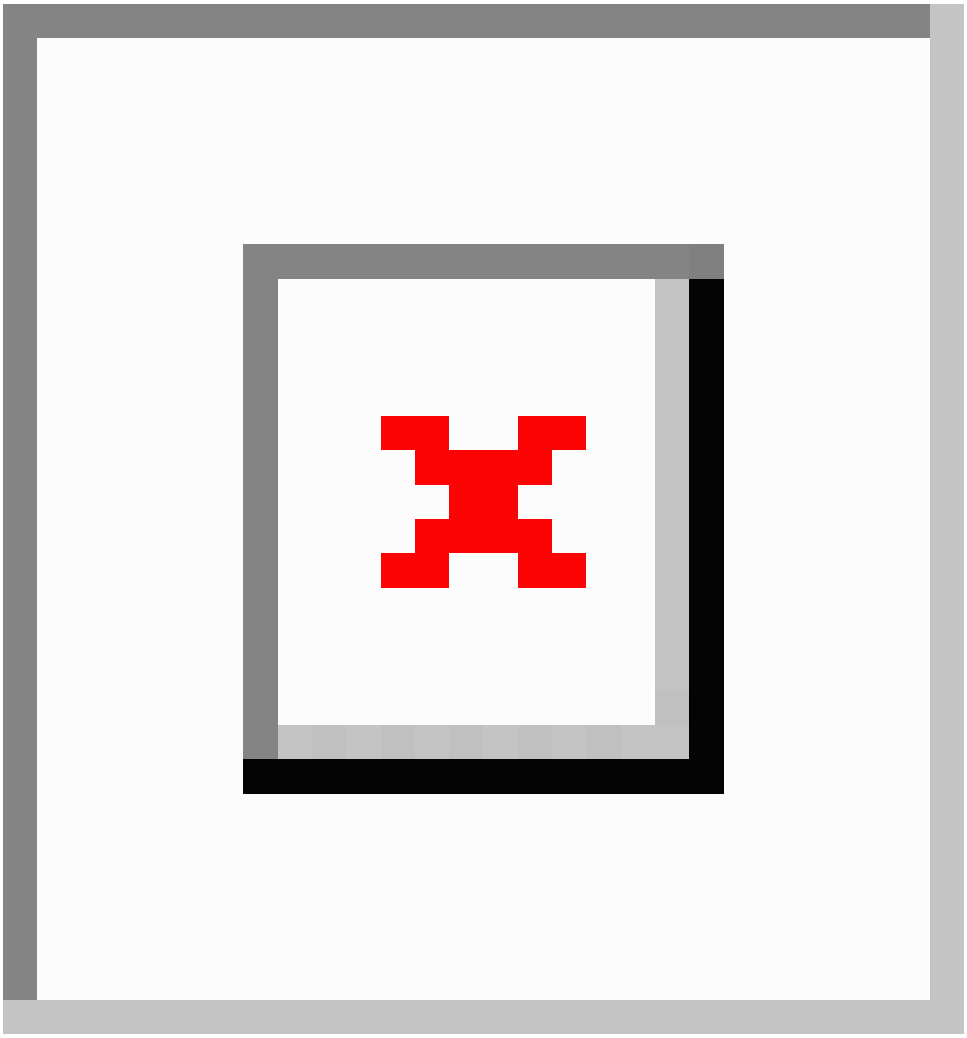
5. L'ASA encapsule de nouveau les paquets avec la balise VXLAN pour VNI 2 et envoie les paquets au serveur virtuel 1. Avant l'encapsulation, l'ASA modifie l'adresse MAC de destination de la trame interne pour qu'elle corresponde à l'adresse MAC de VM1 (l'ARP encapsulé en multidiffusion peut être nécessaire pour que l'ASA apprenne l'adresse MAC de VM1).
6. Lorsque le serveur virtuel 1 reçoit les paquets VXLAN, il désencapsule les paquets et achemine les trames internes à la VM1.

Équilibreur de charge de passerelle AWS et serveur mandataire à un seul volet de Geneve

Remarque Ce scénario est le seul actuellement pris en charge pour les interfaces de Geneve.

L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente et un équilibreur de charge qui répartit le trafic et fait évoluer les périphériques virtuels à la demande. L'ASA Virtual prend en charge le plan de contrôle centralisé de l'équilibreur de charge de passerelle avec un plan de données distribué (point terminal de l'équilibreur de charge de passerelle). La figure suivante montre le trafic acheminé vers l'équilibreur de charge de passerelle à partir du point terminal de l'équilibreur de charge de passerelle. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs ASA Virtual, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle (trafic à demi-tour). L'équilibreur de charge de passerelle renvoie ensuite le trafic au point terminal de l'équilibreur de charge de passerelle et à la destination.

Illustration 77 : Serveur mandataire à un seul volet Geneve

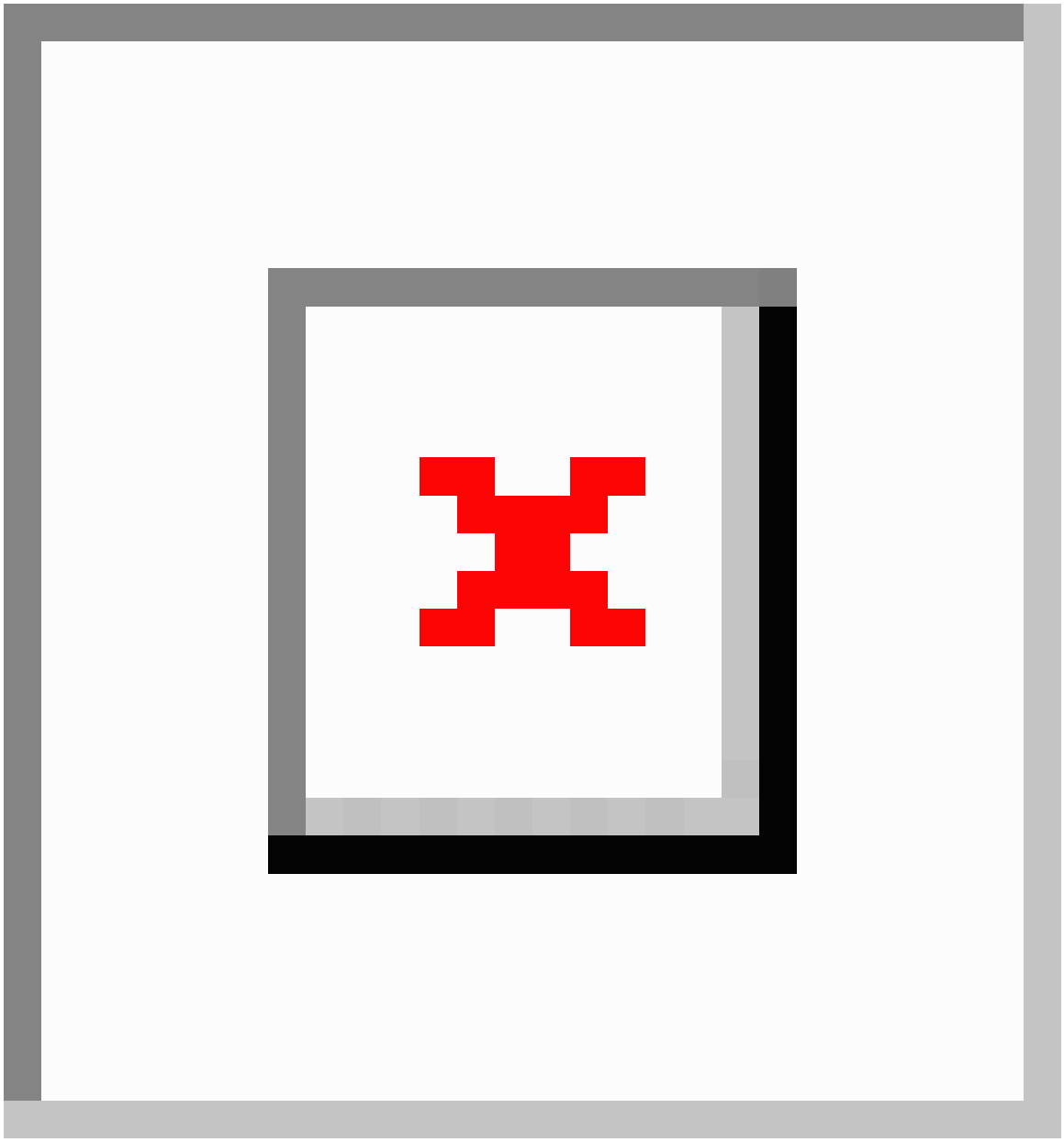


Équilibreur de charge de passerelle Azure et serveur mandataire jumelé

Dans une chaîne de service Azure, les ASA Virtualagissent comme une passerelle transparente qui peut intercepter les paquets entre Internet et le service client. Le ASA Virtual définit une interface externe et une interface interne sur une seule carte réseau en utilisant les segments VXLAN dans un serveur mandataire apparié.

La figure suivante montre le trafic transféré vers l'équilibreur de charge de passerelle Azure à partir de l'équilibreur de charge de passerelle publique sur le segment VXLAN externe. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs ASA Virtual, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle sur le segment VXLAN interne. L'équilibreur de charge de passerelle Azure renvoie ensuite le trafic vers l'équilibreur de charge de passerelle publique et vers la destination.

Illustration 78 : Équilibreur de charge de passerelle Azure avec mandataire jumelé



Exigences et conditions préalables pour les interfaces VXLAN

Exigences du modèle

- Les ports de commutation Firepower 1010 et les interfaces VLAN ne sont pas pris en charge en tant qu'interfaces VTEP.

- L'encapsulation Geneve est prise en charge pour les modèles suivants : ASAv30, ASAv50, ASAv100 sur Amazon Web Services (AWS)
- Le réseau VXLAN en mode proxy jumelé est pris en charge pour les modèles suivants :
  - ASA virtuel dans Azure

Lignes directrices pour les interfaces VXLAN

Mode pare-feu

- Les interfaces Geneve ne sont prises en charge qu'en mode de pare-feu routé.
- Les interfaces VXLAN mandataires jumelées ne sont prises en charge qu'en mode de pare-feu routé.

IPv6

- L'interface VNI prend en charge le trafic IPv4 et IPv6.
- L'adresse IP de l'interface source VTEP prend uniquement en charge IPv4.

Mise en grappe et mode de contexte multiple

- La mise en grappe d'ASA ne prend pas en charge VXLAN en mode d'interface individuelle, sauf pour la liaison de commande de grappe (ASA virtuel seulement). Seul le mode EtherChannel étendu prend en charge VXLAN.

  Une exception est faite pour l'ASA virtuel sur AWS, qui peut utiliser une interface Geneve supplémentaire à utiliser avec GWLB.
- Les interfaces Geneve ne sont prises en charge qu'en mode en mode de contexte unique. Elles ne sont pas prises en charge avec le mode de contexte multiple.

Routage

- Seul le routage statique ou le routage basé sur des politiques est pris en charge sur l'interface VNI; les protocoles de routage dynamique ne sont pas pris en charge.

VPN

Vous ne pouvez pas configurer l'interface source VTEP pour le VPN ou l'utiliser comme VTI.

MTU

- Encapsulation VXLAN : si la MTU de l'interface source est inférieure à 1 554 octets pour IPv4 ou à 1 574 octets pour IPv6 ou 1 574 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Si la MTU utilisée par d'autres périphériques est supérieure, vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 54 octets. Cette MTU nécessite l'activation de la réservation de bâti grand format

sur certains modèles; voir Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000), à la page 618.

- Encapsulation Geneve : si la MTU de l'interface source est inférieure à 1 806 octets, l'ASA fait automatiquement passer la MTU à 1 806 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Si la MTU utilisée par d'autres périphériques est supérieure, vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 306 octets. Cette MTU nécessite l'activation de la réservation de bâti grand format sur certains modèles; voir Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000), à la page 618.

Paramètres par défaut des interfaces VXLAN

Les interfaces VNI sont activées par défaut.

Configurer les interfaces VXLAN

Pour configurer les interfaces VXLAN, procédez comme suit.

Remarque Vous pouvez configurer VXLAN ou Geneve (ASA virtuel uniquement). Pour les interfaces Geneve, consultez Configurer les interfaces Geneve, à la page 683.

Procédure

Étape 1 Configurer l'interface source VTEP, à la page 681.

Étape 2 Configurer l'interface VNI, à la page 682

Étape 3 (Azure GWLB) Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle, à la page 685.

Configurer l'interface source VTEP

Vous pouvez configurer une interface source de VTEP par ASA ou par contexte de sécurité. Le VTEP est défini comme un terminal de virtualisation de réseau (NVE).

Avant de commencer

Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Dans le volet Configuration > Liste des périphériques, double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, et modifiez l'interface que vous souhaitez utiliser pour l'interface source VTEP.

Étape 2 (Mode transparent) Cochez la case **VTEP Source Interface** (Interface source VTEP).

Ce paramètre vous permet de configurer une adresse IP pour l'interface. Cette commande est facultative pour le mode routé où ce paramètre limite le trafic à VXLAN uniquement sur cette interface.

Étape 3 Configurez le nom de l'interface source et l'adresse IPv4 , puis cliquez sur **OK**.

Étape 4 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **VXLAN** .

Étape 5 (Facultatif) Saisissez une valeur dans **VXLAN Destination Port** (Port de destination VXLAN) si vous souhaitez modifier la valeur par défaut de 4789.

En mode de contexte multiple, configurez ce paramètre dans l'espace d'exécution du système.

Étape 6 Dans le menu déroulant **Enable Network Virtualization Endpoint encapsulation** (Activer l'encapsulation du terminal de virtualisation du réseau), choisissez **VXLAN**.

Étape 7 Choisissez l'option **VTEP Tunnel Interface** (Interface de tunnel VTEP) dans la liste déroulante.

Remarque Si la MTU de l'interface VTEP est inférieure à 1 554 octets, l'ASA augmente automatiquement la MTU à 1 554 octets.

Étape 8 (Facultatif) Cochez la case **Configure Packet Recipient** (Configurer le destinataire des paquets).

- (Mode de contexte multiple; facultatif pour le mode unique) Renseignez le champ **Specify Peer VTEP IP Address** (Spécifier l'adresse IP VTEP de l'homologue) pour spécifier manuellement l'adresse IP VTEP de l'homologue

  Si vous spécifiez l'adresse IP de l'homologue, vous ne pouvez pas utiliser la découverte de groupe de multidiffusion. La multidiffusion n'est pas prise en charge en mode de contexte multiple, la configuration manuelle est donc la seule option. Vous ne pouvez définir qu'un seul homologue pour le VTEP.

- (Mode unique seulement) Renseignez le champ **Multicast traffic to default multicast address** (Trafic de multidiffusion vers l'adresse de multidiffusion par défaut) pour spécifier un groupe de multidiffusion par défaut pour toutes les interfaces VNI associées.

  Si vous ne configurez pas le groupe de multidiffusion par interface VNI, ce groupe est utilisé. Si vous configurez un groupe au niveau de l'interface VNI, ce groupe remplace ce paramètre.

Étape 9 Cliquez sur **Apply** (Appliquer).

Configurer l'interface VNI

Ajoutez une interface VNI, associez-la à l'interface source VTEP et configurez les paramètres de l'interface de base.

Pour l'ASA virtuel dans Azure, vous pouvez configurer une interface VXLAN standard ou une interface VXLAN en mode de mandataire jumelé à utiliser avec la GWLB Azure.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres de l'interface)** > **Interfaces** et cliquez sur **Add (Ajouter)** > **VNI Interface (Interface VNI)**.

Étape 2 Saisissez le **VNI ID** (ID VNI) compris entre 1 et 10 000.

Cet ID est simplement un identifiant d'interface interne.

Étape 3 Saisissez le **VNI Segment ID** (ID de segment VNI) compris entre 1 et 16777215.

L'ID de segment est utilisé pour le balisage VXLAN.

Étape 4 (Mode transparent) Choisissez le **Bridge Group** (Groupe de ponts) auquel vous souhaitez affecter cette interface.

Consultez Configurer les interfaces de groupe de ponts, à la page 702 pour configurer l'interface BVI et associer des interfaces standard à ce groupe de ponts.

Étape 5 Saisissez l'**Interface Name** (Nom de l'interface).

Le nom est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur.

Étape 6 Saisissez le **Security Level** (Niveau de sécurité), entre 0 (le plus bas) et 100 (le plus élevé). Consultez Niveaux de sécurité, à la page 694.

Étape 7 (Mode unique) Renseignez le champ **Multicast Group IP Address** (Adresse IP du groupe de multidiffusion).

Si vous ne définissez pas le groupe de multidiffusion pour l'interface VNI, le groupe par défaut de la configuration de l'interface source VTEP est utilisé, s'il est disponible. Si vous définissez manuellement une adresse IP homologue VTEP pour l'interface source de VTEP, vous ne pouvez pas spécifier de groupe de multidiffusion pour l'interface VNI. La multidiffusion n'est pas prise en charge en mode de contexte multiple.

Étape 8 Cochez la case **Map to VTEP Tunnel Interface** (Mapper à l'interface de tunnel VTEP).

Ce paramètre associe l'interface VNI à l'interface source VTEP.

Étape 9 Cochez la case**Enable Interface** (Activer l'interface). Ce paramètre est activé par défaut.

Étape 10 (Mode routé) Dans la zone **IP Address** (Adresse IP), configurez une adresse IPv4. Pour configurer IPv6, cliquez sur l'onglet **IPv6**.

Étape 11 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Configurer les interfaces Geneve

Pour configurer les interfaces de Geneve pour ASA virtuel, procédez comme suit.

Remarque Vous pouvez configurer VXLAN ou Geneve. Pour les interfaces VXLAN, consultez Configurer les interfaces VXLAN, à la page 681.

Procédure

Étape 1 Configurer l'interface source VTEP pour Geneve, à la page 684.

Étape 2 Configurer l'interface VNI pour Geneve, à la page 685

Étape 3 Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle, à la page 685.

Configurer l'interface source VTEP pour Geneve

Vous pouvez configurer une interface source de VTEP par ASA virtuel. Le VTEP est défini comme un point terminal de virtualisation du réseau (NVE).

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, et modifiez l'interface que vous souhaitez utiliser pour l'interface source VTEP.

Étape 2 (Facultatif) Cochez la case **VTEP Source Interface** (Interface source VTEP).

Ce paramètre limite le trafic vers VXLAN uniquement sur cette interface.

Étape 3 Configurez le nom de l'interface source et l'adresse IPv4, puis cliquez sur **OK**.

Étape 4 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **VXLAN** .

Étape 5 Dans le menu déroulant **Enable Network Virtualization Endpoint encapsulation** (Activer l'encapsulation du terminal de virtualisation du réseau), choisissez **Geneve**.

Étape 6 Ne modifiez pas le **port Geneve**; AWS nécessite un port 6081.

Étape 7 Choisissez l'option **VTEP Tunnel Interface** (Interface de tunnel VTEP) dans la liste déroulante.

Remarque Si la MTU de l'interface VTEP est inférieure à 1 806 octets, l'ASA augmente automatiquement la MTU à 1 806 octets.

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer l'interface VNI pour Geneve

Ajoutez une interface VNI, associez-la à l'interface source VTEP et configurez les paramètres de l'interface de base.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres de l'interface)** > **Interfaces** et cliquez sur **Add (Ajouter)** > **VNI Interface (Interface VNI)**.

Étape 2 Saisissez le **VNI ID** (ID VNI) compris entre 1 et 10 000.

Cet ID est simplement un identifiant d'interface interne.

Étape 3 Saisissez l'**Interface Name** (Nom de l'interface).

Le nom est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur.

Étape 4 Saisissez le **Security Level** (Niveau de sécurité), entre 0 (le plus bas) et 100 (le plus élevé). Consultez Niveaux de sécurité, à la page 694.

Étape 5 Cochez la case **Map to VTEP Tunnel Interface** (Mapper à l'interface de tunnel VTEP).

Ce paramètre associe l'interface VNI à l'interface source VTEP.

Étape 6 Cochez la case**Enable Interface** (Activer l'interface). Ce paramètre est activé par défaut.

Étape 7 Cochez la case **Enable Single-Arm Proxy** (Activer le serveur mandataire à un seul volet).

Étape 8 Dans la zone **IP Address** (Adresse IP), configurez une adresse IPv4. Pour configurer IPv6, cliquez sur l'onglet **IPv6**.

Étape 9 Cliquez sur **OK**.

Étape 10 Pour autoriser le trafic à entrer et à sortir de la même interface, cochez la case **Enable traffic between two or more hosts connected to the same interface** (Activer le trafic entre deux hôtes ou plus connectés à la même interface).

Étape 11 Cliquez sur **Apply** (Appliquer).

Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle

L'équilibreur de charges de la passerelle AWS ou Azure nécessite des périphériques pour répondre correctement à une vérification de l'intégrité. L'équilibreur de charges de la passerelle AWS enverra uniquement le trafic vers des périphériques considérés comme intègres.

Vous devez configurer l'ASA virtuel pour répondre à une vérification de l'intégrité SSH, HTTP ou HTTPS.

Connexion SSH

Pour SSH, autorisez SSH à partir de l'équilibreur de charges de la passerelle. L'équilibreur de charges de la passerelle tentera d'établir une connexion à ASA virtuel, et l'invite de connexion de l'ASA virtuel est considérée comme une preuve de l'intégrité.

Remarque Une tentative de connexion SSH expirera après 1 minute. Vous devrez configurer un intervalle de vérification de l'intégrité plus long sur l'équilibreur de charges de la passerelle pour tenir compte de ce délai.

Connexion Telnet

Pour Telnet, autorisez Telnet à partir de l'équilibreur de charges de la passerelle. L'équilibreur de charges de la passerelle tentera d'établir une connexion à ASA virtuel, et l'invite de connexion de l'ASA virtuel est considérée comme une preuve de l'intégrité.

Remarque Vous ne pouvez pas vous connecter via Telnet à l'interface du niveau de sécurité le plus bas, donc cette méthode peut ne pas être pratique.

Mandataire direct HTTP(S)

Vous pouvez configurer l'ASA pour demander à l'équilibreur de charges de la passerelle de vous connecter par HTTP(S).

Redirection HTTP(S) à l'aide de la NAT d'interface statique avec traduction de port

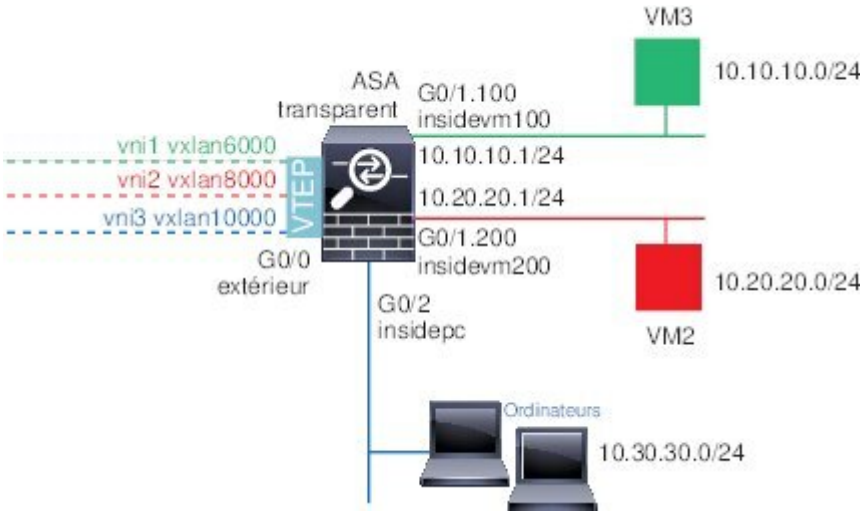
Vous pouvez configurer ASA virtuel pour rediriger les vérifications de l'intégrité vers un serveur HTTP(S) de métadonnées. Pour les vérifications de l'intégrité HTTP(S), le serveur HTTP(S) doit répondre à l'équilibreur de charges de la passerelle avec un code d'état compris entre 200 et 399. Étant donné que l'ASA virtuel a des limites sur le nombre de connexions de gestion simultanées, vous pouvez choisir de décharger le contrôle de l'intégrité sur un serveur externe.

La NAT d'interface statique avec traduction de port vous permet de rediriger une connexion vers un port (comme le port 80) vers une adresse IP différente. Par exemple, traduisez un paquet HTTP de l'équilbreur de charges de la passerele avec la destination de l'interface externe ASA virtuel de sorte qu'il semble provenir de l'interface externe ASA virtuel avec la destination du serveur HTTP. L'ASA virtuel transfère ensuite le paquet vers l'adresse de destination mappée. Le serveur HTTP répond à l'interface externe ASA virtuel, puis ASA virtuel renvoie la réponse à l'équilibreur de charges de la passerelle. Vous avez besoin d'un critère d'accès qui autorise le trafic de l'équilibreur de charges de la passerelle vers le serveur HTTP.

Exemples d'interfaces VXLAN

Consultez les exemples de configuration suivants pour VXLAN.

Exemple de passerelle VXLAN transparente



Consultez la description suivante de cet exemple :

- L'interface externe sur GigabitEthernet 0/0 est utilisée comme interface source VTEP et est connectée au réseau de couche 3.
- La sous-interface VLAN insidevm100 sur GigabitEthernet 0/1.100 est connectée au réseau 10.10.10.0/24, sur lequel réside VM3. Lorsque VM3 communique avec VM1 (non affiché; les deux ont des adresses IP 10.10.10.0/24), l'ASA utilise la balise VXLAN 6000.
- La sous-interface VLAN insidevm200 sur GigabitEthernet 0/1.200 est connectée au réseau 10.20.20.0/24, sur lequel réside VM2. Lorsque VM2 communique avec VM4 (non affiché; les deux ont des adresses IP 10.20.20.0/24), l'ASA utilise la balise VXLAN 8000.
- L'interface insidepc de GigabitEthernet 0/2 est connectée au réseau 10.30.30.0/24 sur lequel se trouvent quelques ordinateurs. Lorsque ces ordinateurs communiquent avec des VM/PC (non affichés) derrière un VTEP distant qui appartient au même réseau (tous ont des adresses IP 10.30.30.0/24), l'ASA utilise la balise VXLAN 10000.

Configuration ASA

```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
```

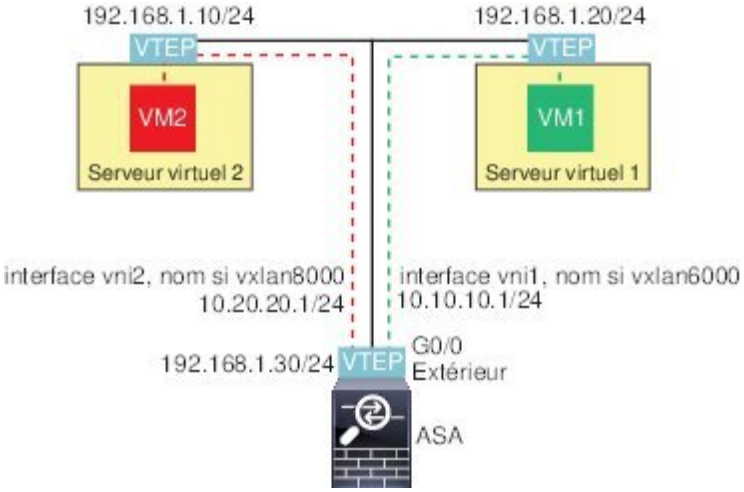
```
  security-level 0
  bridge-group 1
  vtep-nve 1
  mcast-group 235.0.0.100
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  bridge-group 2
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface vni3
  segment-id 10000
  nameif vxlan10000
  security-level 0
  bridge-group 3
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface gigabitethernet0/1.100
  nameif insidevm100
  security-level 100
  bridge-group 1
!
interface gigabitethernet0/1.200
  nameif insidevm200
  security-level 100
  bridge-group 2
!
interface gigabitethernet0/2
  nameif insidepc
  security-level 100
  bridge-group 3
!
interface bvi 1
  ip address 10.10.10.1 255.255.255.0
!
interface bvi 2
  ip address 10.20.20.1 255.255.255.0
!
interface bvi 3
  ip address 10.30.30.1 255.255.255.0
```

Notes

- Pour les interfaces VNI vni1 et vni2, la balise VLAN interne est supprimée pendant l'encapsulation.
- Les interfaces VNI vni2 et vni3 partagent la même adresse IP de multidiffusion pour l'ARP encapsulé sur la multidiffusion. Ce partage est autorisé.
- L'ASA relie le trafic VXLAN vers des interfaces non prises en charge par VXLAN en fonction des BVI et des configurations de groupes de ponts ci-dessus. Pour chacun des segments de réseau étendus de couche 2 (10.10.10.0/24, 10.20.20.0/24 et 10.30.30.0/24), l'ASA sert de pont.
- Il est autorisé d'avoir plusieurs VNI ou plusieurs interfaces standard (VLAN ou simplement interface physique) dans un groupe de ponts. Le transfert ou l'association entre l'ID de segment VXLAN et l'ID de VLAN (ou une interface physique) est décidé par l'adresse MAC de destination et l'interface qui se connecte à la destination.

- L'interface source VTEP est une interface de couche 3 en mode de pare-feu transparent, indiquée par **nve-only** dans la configuration de l'interface. L'interface source VTEP n'est pas une interface BVI ni une interface de gestion, mais elle a une adresse IP et utilise la table de routage.

Exemple de routage VXLAN



Consultez la description suivante de cet exemple :

- VM1 (10.10.10.10) est hébergé sur le serveur virtuel 1 et VM2 (10.20.20.20) est hébergé sur le serveur virtuel 2.
- La passerelle par défaut pour VM1 est l'ASA, qui ne se trouve pas dans le même module que le serveur virtuel 1, mais VM1 ne le sait pas. VM1 sait uniquement que l'adresse IP de sa passerelle par défaut est 10.10.10.1. De même, VM2 sait uniquement que l'adresse IP de sa passerelle par défaut est 10.20.20.1.
- Les hyperviseurs pris en charge par le VTEP sur les serveurs virtuels 1 et 2 peuvent communiquer avec l'ASA sur le même sous-réseau ou par l'intermédiaire d'un réseau de couche 3 (non illustré; dans ce cas, l'ASA et les liaisons ascendantes des serveurs virtuels ont des adresses réseau différentes).
- Le paquet de VM1 sera encapsulé par le VTEP de son hyperviseur et envoyé à sa passerelle par défaut sur la tunnellisation VXLAN.
- Lorsque VM1 envoie un paquet à VM2, le paquet sera envoyé par la passerelle par défaut 10.10.10.1 de son point de vue. Le serveur virtuel 1 sait que la passerelle 10.10.10.1 n'est pas locale; par conséquent, le VTEP encapsule le paquet sur VXLAN et l'envoie au VTEP de l'ASA.
- Sur l'ASA, le paquet est désencapsulé. L'ID de segment VXLAN est appris lors de la désencapsulation. L'ASA réinjecte ensuite le cadre interne dans l'interface VNI (vni1) correspondante en fonction de l'ID de segment VXLAN. L'ASA effectue ensuite une recherche de route et envoie le paquet interne par une autre interface VNI, vni2. Tous les paquets sortants par vni2 sont encapsulés avec le segment VXLAN 8000 et envoyés par le VTEP à l'extérieur.
- Finalement, le paquet encapsulé est reçu par le VTEP du serveur virtuel 2, qui le désencapsule et le transfère à VM2.

Configuration ASA

```
interface gigabitethernet0/0
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
  default-mcast-group 235.0.0.100
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  vtep-nve 1
  ip address 10.20.20.1 255.255.255.0
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  vtep-nve 1
  ip address 10.10.10.1 255.255.255.0
!
```

Historique des interfaces VXLAN

Tableau 32 : Historique des interfaces VXLAN

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Proxy jumelé VXLAN pour l'ASA virtuel pour l'équilibreur de charges de la passerelle Azure.	9.19(1)	Vous pouvez configurer une interface VXLAN en mode proxy apparié pour l'ASA virtuel dans Azure afin de l'utiliser avec l'équilibreur de charges de la passerelle Azure (GWLB). L'ASA virtuel définit une interface externe et une interface interne sur un seul NIC en utilisant des segments VXLAN dans un serveur mandataire jumelé. Commandes nouvelles/modifiées : **port externe, segment-id externe, port interne, segment-id interne, proxy paired** ASDM n'est pas pris en charge.
Prise en charge de Geneve pour l'ASA virtuel sur AWS pour l'équilibreur de charges de la passerelle AWS	9.17(1)	La prise en charge de l'encapsulation Geneve a été ajoutée pour l'ASAv30, ASAv50 et ASAv100 afin de prendre en charge le serveur mandataire à un seul volet pour l'équilibreur de charges de passerelle AWS. Écrans Nouveaux ou modifiés : **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add (Ajouter) > VNI Interface (Interface VNI)** **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > VXLAN**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de VXLAN	9.4(1)	La prise en charge de VXLAN a été ajoutée, y compris la prise en charge du terminal de tunnel VXLAN (VTEP). Vous pouvez définir une interface source VTEP par ASA ou contexte de sécurité. Nous avons introduit les écrans suivants : **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add (Ajouter) > VNI Interface (Interface VNI)** **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > VXLAN**



CHAPITRE 21

Interfaces en mode routage et en mode transparent

Ce chapitre comprend des tâches pour terminer la configuration de l'interface pour tous les modèles en mode de pare-feu routé ou transparent.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Dans le volet Configuration > Liste des périphériques, double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

- À propos des interfaces en mode routage et en mode transparent, à la page 693
- Directives et limites pour les interfaces en mode routé et en mode transparent, à la page 695
- Configurer les interfaces en mode routé, à la page 698
- Configurer les interfaces de groupe de ponts, à la page 702
- Configuration de l'adressage IPv6, à la page 707
- Supervision des interfaces en mode routé et en mode transparent, à la page 720
- Exemples d'interfaces en mode routé et en mode transparent, à la page 723
- Historique des interfaces en mode routé et en mode transparent, à la page 726

À propos des interfaces en mode routage et en mode transparent

L'ASA prend en charge deux types d'interfaces : routées et pontées.

Chaque interface routée de couche 3 nécessite une adresse IP sur un sous-réseau unique.

Les interfaces pontées appartiennent à un groupe de ponts et toutes les interfaces se trouvent sur le même réseau. Le groupe de ponts est représenté par une interface virtuelle de pont (BVI) qui a une adresse IP sur le réseau de ponts. Le mode routé prend en charge les interfaces routées et pontées, et vous pouvez effectuer le routage entre des interfaces routées et des BVI. Le mode de pare-feu transparent ne prend en charge que les interfaces de groupe de ponts et BVI.

Niveaux de sécurité

Chaque interface doit avoir un niveau de sécurité de 0 (le plus bas) à 100 (le plus élevé), y compris les interfaces membres d'un groupe de ponts. Par exemple, vous devez affecter votre réseau le plus sécurisé, comme le réseau d'hôte interne, au niveau 100. Le réseau externe connecté à Internet peut quant à lui être attribué au niveau 0. D'autres réseaux, tels que les DMZ, peuvent être entre les deux. Vous pouvez attribuer des interfaces au même niveau de sécurité.

L'attribution d'un niveau de sécurité à une BVI dépend du mode de pare-feu. En mode transparent, l'interface BVI n'a pas de niveau de sécurité, car elle ne participe pas au routage entre les interfaces. En mode routé, les interfaces BVI ont un niveau de sécurité si vous choisissez d'effectuer le routage entre les BVI et d'autres interfaces. Pour le mode routé, le niveau de sécurité d'une interface membre d'un groupe de ponts s'applique uniquement à la communication au sein du groupe de ponts. De même, le niveau de sécurité BVI s'applique uniquement à la communication inter-BVI/interface de couche 3.

Le niveau contrôle le comportement suivant :

- Accès au réseau : par défaut, il existe une autorisation implicite d'une interface de sécurité supérieure vers une interface de sécurité inférieure (sortante). Les hôtes de l'interface de sécurité supérieure peuvent accéder à n'importe quel hôte sur une interface de sécurité inférieure. Vous pouvez limiter l'accès en appliquant une ACL à l'interface.

  Si vous activez la communication pour des interfaces de même sécurité, il existe une autorisation implicite pour que les interfaces accèdent à d'autres interfaces sur le même niveau de sécurité ou un niveau de sécurité inférieur.

- Moteurs d'inspection : certains moteurs d'inspection d'applications dépendent du niveau de sécurité. Pour les interfaces de même sécurité, les moteurs d'inspection s'appliquent au trafic dans l'une ou l'autre direction.
  - Plateforme d'inspection NetBIOS : s'applique uniquement aux connexions sortantes.
  - Plateforme d'inspection SQL*Net : si une connexion de contrôle pour le port SQL*Net (anciennement OraServ) existe entre une paire d'hôtes, seule une connexion de données entrante est autorisée par l'ASA.

Double pile IP (IPv4 et IPv6)

L'ASA prend en charge les adresses IPv6 et IPv4 sur une interface. Assurez-vous de configurer une voie de routage par défaut pour IPv4 et IPv6.

Masque de sous-réseau 31 bits

Pour les interfaces routées, vous pouvez configurer une adresse IP sur un sous-réseau de 31 bits pour les connexions point à point. Le sous-réseau de 31 bits comprend seulement 2 adresses; normalement, la première et la dernière adresse du sous-réseau sont réservées pour le réseau et la diffusion, donc un sous-réseau à deux adresses n'est pas utilisable. Toutefois, si vous avez une connexion point à point et n'avez pas besoin d'adresses de réseau ou de diffusion, un sous-réseau de 31 bits est un moyen utile de conserver les adresses dans IPv4. Par exemple, la liaison de basculement entre 2 ASA ne nécessite que 2 adresses; les paquets transmis par une extrémité de la liaison sont toujours reçus par l'autre extrémité, et la diffusion n'est pas nécessaire. Vous pouvez également avoir une station de gestion directement connectée exécutant SNMP ou Syslog.

Sous-réseau 31 bits et mise en grappe

Vous pouvez utiliser un masque de sous-réseau de 31 bits de grappe en mode de mise en grappe étendue, à l'exclusion de l'interface de gestion et de la liaison de commande de grappe.

Vous ne pouvez pas utiliser un masque de sous-réseau de 31 bits en mode de mise en grappe individuelle sur une interface.

Sous-réseau 31 bits et basculement

Pour le basculement, lorsque vous utilisez un sous-réseau de 31 bits pour l'adresse IP d'interface ASA, vous ne pouvez pas configurer d'adresse IP de secours pour l'interface, car il n'y a pas assez d'adresses. Normalement, une interface de basculement doit avoir une adresse IP de secours pour que l'unité active puisse effectuer des tests d'interface pour s'assurer de l'intégrité de l'interface de secours. Sans adresse IP de secours, ASA ne peut effectuer aucun test de réseau. seul l'état du lien peut être suivi.

Pour le basculement et le lien à état séparé facultatif, qui sont des connexions point à point, vous pouvez également utiliser un sous-réseau de 31 bits.

Gestion et sous-réseau 31 bits

Si vous avez une station de gestion directement connectée, vous pouvez utiliser une connexion point à point pour SSH ou HTTP sur ASA, ou pour SNMP ou Syslog sur le poste de gestion.

Fonctionnalités 31 bits non prises en charge

Les fonctionnalités suivantes ne prennent pas en charge le sous-réseau de 31 bits :

- Interfaces BVI pour les groupes de ponts : le groupe de ponts nécessite au moins 3 adresses d'hôte : les BVI et deux hôtes connectés à deux interfaces membres du groupe de ponts. vous devez utiliser un sous-réseau /29 ou moins.
- Routage multidiffusion

Directives et limites pour les interfaces en mode routé et en mode transparent

Mode contextuel

- En mode de contexte multiple, vous pouvez seulement configurer les interfaces de contexte que vous avez déjà affectées au contexte dans la configuration système en fonction de Configurer plusieurs contextes, à la page 269.
- PPPoE n'est pas pris en charge en mode de contexte multiple.
- Pour le mode à contextes multiples en mode transparent, chaque contexte doit utiliser des interfaces différentes; vous ne pouvez pas partager une interface entre contextes.
- Pour le mode à contexte multiple en mode transparent, chaque contexte utilise généralement un sous-réseau différent. Vous pouvez utiliser des sous-réseaux qui se chevauchent, mais la topologie de votre réseau nécessite une configuration de routeur et de NAT pour que cela soit possible du point de vue du routage.

- Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode de contexte multiple.
- En mode de pare-feu routé, les interfaces de groupes de ponts ne sont pas prises en charge dans le mode de contexte multiple.

Basculement, mise en grappe

- Ne configurez pas les liens de basculement selon les procédures de ce chapitre. Consultez le chapitre Basculement pour plus de renseignements.
- Pour les interfaces de grappe, consultez le chapitre sur la mise en grappe pour connaître les exigences.
- Lorsque vous utilisez Basculement, vous devez définir l'adresse IP et l'adresse de secours pour les interfaces de données manuellement. DHCP et PPPoE ne sont pas pris en charge.

IPv6

- IPv6 est pris en charge sur toutes les interfaces.
- Vous ne pouvez que configurer les adresses IPv6 manuellement en mode transparent.
- L'ASA ne prend pas en charge les adresses anycast IPv6.
- Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode à contexte multiple, le mode transparent, la mise en grappe ou Basculement.

Directives sur les modèles

- Pour l’ASAv50, les groupes de ponts ne sont pas pris en charge en mode transparent ou routé.
- Pour les périphériques Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.

Directives relatives au mode transparent et au groupe de ponts

- Vous pouvez créer jusqu’à 250 groupes de ponts, avec interfaces par groupe de ponts.
- Chaque réseau connecté directement doit se trouver sur le même sous-réseau.
- L'ASA ne prend pas en charge le trafic sur les réseaux secondaires; seul le trafic sur le même réseau que l’adresse IP BVI est pris en charge.
- Une adresse IP pour les BVI est requise pour chaque groupe de ponts pour le trafic de gestion vers le périphérique et en provenance du périphérique, ainsi que pour le trafic de données qui doit passer par ASA. Pour le trafic IPv4, spécifiez une adresse IPv4. Pour le trafic IPv6, spécifiez une adresse IPv6.
- Vous ne pouvez configurer les adresses IPv6 que manuellement.
- L’adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Vous ne pouvez pas définir le sous-réseau comme sous-réseau d’hôte (255.255.255.255).
- Les interfaces de gestion ne sont pas prises en charge en tant que membres de groupes de ponts.
- Pour l’ASAv50 sur VMware avec des interfaces ixgbevf pontées, le mode transparent n’est pas pris en charge et les groupes de ponts ne sont pas pris en charge en mode routé.

- Pour Série Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour le 200/ 1010/ , il n'est pas possible de mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques au sein du même groupe de ponts.
- En mode transparent, vous devez utiliser au moins un groupe de ponts; les interfaces de données doivent appartenir à un groupe de ponts.
- En mode transparent, ne spécifiez pas l'adresse IP des BVI comme passerelle par défaut pour les périphériques connectés; Les périphériques doivent spécifier le routeur de l'autre côté de la ASA comme passerelle par défaut.
- En mode transparent, la voie de routage *par défaut*, qui est requise pour fournir un chemin de retour au trafic de gestion, n'est appliquée qu'au trafic de gestion provenant d'un réseau de groupe de ponts. En effet, la voie de routage par défaut spécifie une interface dans le groupe de ponts ainsi que l'adresse IP du routeur sur le réseau du groupe de ponts, et vous ne pouvez définir qu'une seule voie de routage par défaut. Si votre trafic de gestion provient de plus d'un réseau de groupes de ponts, vous devez spécifier une voie de routage statique régulière qui identifie le réseau à partir duquel vous attendez le trafic de gestion.
- Le protocole PPPoE n'est pas pris en charge sur l'interface Management (gestion).
- En mode routé, pour le routage entre les groupes de ponts et les autres interfaces routées, vous devez nommer les BVI.
- En mode routé, les interfaces EtherChannel définies par ASA et VNI ne sont pas prises en charge en tant que membres de groupes de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.
- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de l'ASA lors de l'utilisation de membres de groupe de ponts. S'il y a deux voisins de chaque côté de l'ASA exécutant BFD, alors l'ASA abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.

Niveau de sécurité par défaut

Le niveau de sécurité par défaut est 0. Si vous nommez une interface « intérieur » et que vous ne définissez pas explicitement le niveau de sécurité, l'ASA le définit à 100.

Remarque Si vous modifiez le niveau de sécurité d'une interface et que vous ne souhaitez pas attendre que les connexions existantes expirent avant d'utiliser les nouveaux renseignements sur la sécurité, vous pouvez effacer les connexions à l'aide de la commande **clear conn**.

Directives et exigences supplémentaires

- L'ASA ne prend en charge qu'un seul en-tête 802.1Q par paquet et ne prend pas en charge plusieurs en-têtes (appelé prise en charge Q-in-Q).
- Des problèmes d'interface, tels que de fréquents changements d'état haut/bas, peuvent empêcher la minuterie de connexion flottante de s'appliquer correctement aux connexions passant par l'interface. Si vous avez des problèmes avec l'état d'une interface, pensez à effacer toutes les connexions une fois que l'état est stabilisé afin de supprimer les connexions non valides.

Configurer les interfaces en mode routé

Pour configurer les interfaces en mode routé, procédez comme suit.

Configurer les paramètres généraux de l'interface en mode routé

Cette procédure décrit comment définir le nom, le niveau de sécurité, l'adresse IPv4 et d'autres options.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List, double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Choisissez la ligne d'interface, puis cliquez sur modifier (**Edit**).

La boîte de dialogue **Edit Interface** (modifier l'interface) s'affiche sous l'onglet **General** (général).

Remarque Pour le Firepower 1010, vous ne pouvez pas configurer de ports de commutation en tant qu'interfaces en mode routé.

Étape 3 Dans le champ **Interface Name** (Nom d'interface), saisissez un nom renfermant au maximum 48 caractères.

Étape 4 Dans le champ **Security level** (Niveau de sécurité), saisissez un niveau compris entre 0 (le plus bas) et 100 (le plus élevé).

Remarque Pour les interfaces de boucle avec retour, vous ne définissez pas de niveau de sécurité, car l'interface n'est prise en charge que pour le trafic vers/depuis le périphérique.

Étape 5 (Facultatif) Pour définir cette interface comme une interface de gestion uniquement, cochez la case **Dedicate this interface to management-only** (Dédier cette interface à la gestion uniquement).

Le trafic de transit n'est pas accepté sur une interface de gestion uniquement.

Remarque Le champ Channel Group (Groupe de canaux) est en lecture seule et indique si l'interface fait partie d'un EtherChannel.

Remarque Pour les interfaces de boucle avec retour, vous ne définissez pas le mode de gestion, car l'interface n'est prise en charge que pour le trafic vers/depuis le périphérique.

Étape 6 Si l'interface n'est pas déjà activée, cochez la case **Enable Interface** (Activer l'interface).

Étape 7 Pour définir l'adresse IP, utilisez l'une des options suivantes.

Remarque Pour le basculement et la mise en grappe, ainsi que pour les interfaces de boucle avec retour, vous devez définir l'adresse IP manuellement; les protocoles DHCP et PPPoE ne sont pas pris en charge.

- Pour définir l'adresse IP manuellement, cliquez sur le bouton radio **Use Static IP** (Utiliser l'adresse IP statique) et saisissez l'adresse IP et le masque.

  Pour le basculement, définissez les adresses IP de veille dans l'onglet **Configuration > Device Management (Gestion des périphériques) > High Availability (Haute disponibilité) > Failover (Basculement) > Interfaces**. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.

  Pour les connexions point à point, vous pouvez spécifier un filtre d'adresse locale de 31 bits (255.255.255.254). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion. Vous ne pouvez pas définir l'adresse IP de secours dans ce cas.
- Pour obtenir une adresse IP d'un serveur DHCP, cliquez sur le bouton radio **Obtain Address via DHCP** (Obtenir l'adresse par DHCP).

  1. Pour forcer le stockage d'une adresse MAC dans un paquet de demande DHCP pour l'option 61, cliquez sur le bouton radio **Use MAC Address** (Utiliser l'adresse MAC).

     Certains fournisseurs de services Internet s'attendent à ce que l'option 61 soit l'adresse MAC de l'interface. Si l'adresse MAC n'est pas incluse dans le paquet de demande DHCP, aucune adresse IP ne sera attribuée.

  2. Pour utiliser une chaîne générée pour l'option 61, cliquez sur **Use "Cisco-<MAC>-<interface_name>-<host>"** (Utiliser « Cisco-<MAC>-<interface_name>-<host> »).

  3. (Facultatif) Pour obtenir la route par défaut à partir du serveur DHCP, cochez **Obtain Default Route Using DHCP** (Obtenir la route par défaut en utilisant DHCP).

  4. (Facultatif) Pour attribuer une distance administrative à la route apprise, saisissez une valeur comprise entre 1 et 255 dans le champ **DHCP Learned Route Metric** (Mesure de route apprise par DHCP). Si ce champ est laissé vide, la distance administrative pour les routes apprises est de 1.

  5. (Facultatif) Pour activer le suivi des routes apprises par DHCP, cochez la case **Enable Tracking for DHCP Learned Routes** (Activer le suivi des routes apprises par DHCP). Définissez les paramètres suivants :

     Track ID (ID de suivi) : identifiant unique pour le processus de suivi de routage. Cette valeur peut être comprise entre 1 et 500.

     Track IP Address (Suivre l'adresse IP) : saisissez l'adresse IP de la cible suivie. En règle générale, il s'agit de l'adresse IP de la passerelle de saut suivant pour le routage, mais il peut s'agir de tout objet réseau disponible à partir de cette interface.

Remarque Le suivi de routage n'est disponible qu'en mode routé unique.

SLA ID (ID de SLA) : identifiant unique pour le processus de supervision des SLA. Cette valeur peut être comprise entre 1 et 2147483647.

Monitor Options (Options de surveillance) : cliquez sur ce bouton pour ouvrir la boîte de dialogue **Route Monitoring Options** (Options de surveillance du routage). Dans la boîte de dialogue **Route Monitoring Options** (Options de surveillance du routage), vous pouvez configurer les paramètres du processus de surveillance des objets suivis.

6. (Facultatif) Pour définir l'indicateur de diffusion sur 1 dans l'en-tête de paquet DHCP, lorsque le client DHCP envoie une découverte demandant une adresse IP, cochez la case **Enable DHCP Broadcast flag for DHCP request and discover messages** (Activer l'indicateur de diffusion DHCP pour les demandes DHCP et les messages de découverte).

   Le serveur DHCP écoute cet indicateur de diffusion et diffuse le paquet de réponse si l'indicateur est défini sur 1.

7. (Facultatif) Pour renouveler le bail locatif, cliquez sur **Renew DHCP Lease** (Renouveler le bail locatif DHCP).

- (Mode unique seulement) Pour obtenir une adresse IP en utilisant PPPoE, cochez la case **Use PPPoE** (Utiliser PPPoE).

  1. Dans le champ **Group Name** (Nom de groupe), indiquez un nom de groupe.
  2. Dans le champ **PPPoE Username** (Nom d'utilisateur PPPoE), spécifiez le nom d'utilisateur fourni par votre FAI.
  3. Dans le champ **PPPoE Password** (Mot de passe PPPoE), spécifiez le mot de passe fourni par votre FAI.
  4. Dans le champ **Confirm Password** (Confirmer le mot de passe), retapez le mot de passe.
  5. Pour l'authentification PPP, cliquez sur le bouton radio **PAP**, **CHAP** ou **MSCHAP**.

     Le PAP transmet un nom d'utilisateur et un mot de passe en clair lors de l'authentification et n'est pas sécurisé. Avec le protocole CHAP, le client renvoie le [défi plus mot de passe] chiffré, avec un nom d'utilisateur en texte clair en réponse au défi du serveur. Le protocole CHAP est plus sécurisé que le protocole PAP, mais il ne chiffre pas les données. MSCHAP est similaire à CHAP, mais est plus sécurisé, car le serveur stocke et compare uniquement les mots de passe chiffrés plutôt que les mots de passe en clair comme dans CHAP. MSCHAP génère également une clé pour le chiffrement des données par MPPE.

  6. (Facultatif) Pour stocker le nom d'utilisateur et le mot de passe dans la mémoire flash, cochez la case **Store Username and Password in Local Flash** (Enregistrer le nom d'utilisateur et le mot de passe dans la mémoire flash locale).

     L'ASA stocke le nom d'utilisateur et le mot de passe dans un emplacement spécial de la NVRAM. Si un Auto Update Server envoie une commande **clear configure** à l'ASA et que la connexion est interrompue, l'ASA peut lire le nom d'utilisateur et le mot de passe de NVRAM et s'authentifier de nouveau auprès du concentrateur d'accès.

7. (Facultatif) Pour afficher la boîte de dialogue **PPPoE IP Address and Route Settings** (Paramètres d'adresse IP et de routage PPPoE) dans laquelle vous pouvez choisir les options d'adressage et de suivi, cliquez sur **IP Address and Route Settings** (Paramètres d'adresse IP et de routage).

Étape 8 (Facultatif) Dans le champ **Description**, saisissez une description pour cette interface.

La description peut contenir jusqu'à 240 caractères sur une seule ligne (sans retour chariot). Dans le cas d'une liaison de basculement ou d'état, la description fixe est « LAN Failover Interface », « STATE Failover Interface » ou « LAN/STATE Failover Interface » par exemple. Vous ne pouvez pas modifier cette description. La description fixe remplace toute description que vous saisissez ici si vous faites de cette interface une liaison de basculement ou un lien d'état.

Étape 9 Cliquez sur **OK**.

Sujets connexes

Configuration de l'adressage IPv6, à la page 707
Activer l'interface physique et configurer les paramètres Ethernet, à la page 615
Configurer le protocole PPPoE, à la page 701

Configurer le protocole PPPoE

Si l'interface est connectée à une liaison ADSL, à un modem câble ou à une autre connexion à votre FAI et que ce dernier utilise PPPoE pour vous fournir votre adresse IP, configurez les paramètres suivants.

Procédure

Étape 1 Choisissez **Configuration** > **Interfaces** > **Add/Edit Interface (Ajouter/Modifier une interface)** > **General (Général)**, puis cliquez sur **PPPoE IP Address and Route Settings (Paramètres de route et d'adresse IP PPPoE)**.

Étape 2 Dans la zone **IP Address** (Adresse IP), choisissez l'une des options suivantes :

- **Obtain IP Address using PPP** (Obtenir l'adresse IP en utilisant PPP) : configurez l'adresse IP de manière dynamique.
- **Specify an IP Address** (Spécifier une adresse IP) : configurez manuellement l'adresse IP.

Étape 3 Dans la zone **Route Settings** (Paramètres de routage), configurez les éléments suivants :

- **Obtain default route using PPPoE** (Obtenir la route par défaut à l'aide de PPPoE) : définissez les routes par défaut lorsque le client PPPoE n'a pas encore établi de connexion. Lorsque vous utilisez cette option, vous ne pouvez pas avoir de route définie de manière statique dans la configuration.
- **PPPoE learned route metric** (Mesure de la route apprise à l'aide de PPPoE) : attribuez une distance administrative à la route apprise. Cette valeur peut être comprise entre 1 et 255. Si ce champ est laissé vide, la distance administrative pour les routes apprises est de 1.
- **Enable tracking** (Activer le suivi) : activez le suivi de routage pour les routes apprises à l'aide de PPPoE. Le suivi de routage n'est disponible qu'en mode routé unique.
- **Primary Track** (Suivi principal) : configurez le suivi de routage PPPoE principal.

- **Track ID** (ID de suivi) : identifiant unique pour le processus de suivi de routage. Cette valeur peut être comprise entre 1 et 500.
- **Track IP Address** (Suivre l'adresse IP) : saisissez l'adresse IP de la cible suivie. En règle générale, il s'agit de l'adresse IP de la passerelle de saut suivant pour le routage, mais il peut s'agir de tout objet réseau disponible à partir de cette interface.
- **SLA ID** (ID de SLA) : identifiant unique pour le processus de supervision des SLA. Cette valeur peut être comprise entre 1 et 2147483647.
- **Monitor Options** (Options de surveillance) : cliquez sur ce bouton pour ouvrir la boîte de dialogue **Route Monitoring Options** (Options de surveillance du routage). Dans la boîte de dialogue **Route Monitoring Options** (Options de surveillance du routage), vous pouvez configurer les paramètres du processus de surveillance des objets suivis.
- **Secondary Track** (Suivi secondaire) : configurez le suivi de routage PPPoE secondaire.
- **Secondary Track ID** (ID de suivi secondaire) : identifiant unique pour le processus de suivi de routage. Cette valeur peut être comprise entre 1 et 500.

Étape 4 Cliquez sur **OK**.

Configurer les interfaces de groupe de ponts

Un groupe de ponts est un groupe d'interfaces que ASA relie par des ponts au lieu de routes. Les groupes de ponts sont pris en charge à la fois en mode transparent et en mode pare-feu routé. Pour en savoir plus sur les groupes de ponts, consultez Groupes de ponts, à la page 221.

Pour configurer des groupes de ponts et les interfaces associées, procédez comme suit.

Configurer la BVI (Bridge Virtual Interface)

Chaque groupe de ponts nécessite un BVI pour lequel vous configurez une adresse IP. L'ASA utilise cette adresse IP comme adresse source pour les paquets provenant du groupe de ponts. L'adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Pour le trafic IPv4, l'adresse IP BVI est requise pour laisser passer le trafic. Pour le trafic IPv6, vous devez, au minimum, configurer les adresses de lien locales pour laisser passer le trafic, mais une adresse de gestion globale est recommandée pour les fonctionnalités complètes, y compris la gestion à distance et d'autres opérations de gestion.

Pour le mode routé, si vous fournissez un nom pour les BVI, alors les BVI participent au routage. Sans nom, le groupe de ponts reste isolé comme en mode transparent de pare-feu.

Certains modèles incluent un groupe de ponts et une BVI dans la configuration par défaut. Vous pouvez créer des groupes de ponts et des BVI supplémentaires et réaffecter des interfaces membres entre les groupes.

Remarque Pour une interface de gestion distincte en mode transparent (pour les modèles pris en charge), un groupe de ponts non configurables (ID 301) est automatiquement ajouté à votre configuration. Ce groupe de ponts n'est pas inclus dans la limite de groupes de ponts.

Procédure

Étape 1 Choisissez **Configuration** > **Interfaces**, puis **Add (Ajouter)** > **Bridge Group Interface (Interface de groupe de pont)**.

Étape 2 Dans le champ **Bridge Group ID** (ID de groupe de ponts), saisissez un ID de groupe de ponts compris entre 1 et 250.

Vous attribuerez ultérieurement des interfaces physiques à ce numéro de groupe de ponts.

Étape 3 (Mode routé) Dans le champ **Interface Name** (Nom d'interface), saisissez un nom de 48 caractères maximum.

Vous devez nommer le BVI si vous souhaitez acheminer le trafic extérieur aux membres du groupe de pont, par exemple vers l'interface externe ou vers les membres d'autres groupes de pont.

Étape 4 (Mode routé) Dans le champ **Security level** (Niveau de sécurité), saisissez un niveau compris entre 0 (le plus bas) et 100 (le plus élevé).

Étape 5 (Mode transparent) Définissez l'adresse IP.

a) Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IPv4.

b) Dans le champ **Subnet Mask** (Filtre d'adresse locale), saisissez le filtre d'adresse locale ou choisissez-en un dans le menu.

N'affectez pas d'adresse hôte (/32 ou 255.255.255.255) au pare-feu transparent. De plus, n'utilisez pas d'autres sous-réseaux contenant moins de 3 adresses d'hôte (une pour le routeur en amont, le routeur en aval et le pare-feu transparent), comme un sous-réseau /30 (255.255.255.252). L'ASA abandonne tous les paquets ARP en provenance ou à destination de la première et de la dernière adresse d'un sous-réseau. Par exemple, si vous utilisez un sous-réseau /30 et que vous affectez une adresse réservée de ce sous-réseau au routeur en amont, l'ASA abandonne la demande ARP du routeur en aval au routeur en amont.

Étape 6 (Mode routé) Pour définir l'adresse IP, utilisez l'une des options suivantes.

Pour le basculement et la mise en grappe, vous devez définir l'adresse IP manuellement; le protocole DHCP n'est pas pris en charge.

- Pour définir l'adresse IP manuellement, cliquez sur le bouton radio **Use Static IP** (Utiliser l'adresse IP statique) et saisissez l'adresse IP et le masque.
- Pour obtenir une adresse IP d'un serveur DHCP, cliquez sur le bouton radio **Obtain Address via DHCP** (Obtenir l'adresse par DHCP).

  1. Pour forcer le stockage d'une adresse MAC dans un paquet de demande DHCP pour l'option 61, cliquez sur le bouton radio **Use MAC Address** (Utiliser l'adresse MAC).

     Certains fournisseurs de services Internet s'attendent à ce que l'option 61 soit l'adresse MAC de l'interface. Si l'adresse MAC n'est pas incluse dans le paquet de demande DHCP, aucune adresse IP ne sera attribuée.

  2. Pour utiliser une chaîne générée pour l'option 61, cliquez sur **Use "Cisco-<MAC>-<interface_name>-<host>"** (Utiliser « Cisco-<MAC>-<interface_name>-<host> »).

  3. (Facultatif) Pour obtenir la route par défaut à partir du serveur DHCP, cochez **Obtain Default Route Using DHCP** (Obtenir la route par défaut en utilisant DHCP).

  4. (Facultatif) Pour définir l'indicateur de diffusion sur 1 dans l'en-tête de paquet DHCP, lorsque le client DHCP envoie une découverte demandant une adresse IP, cochez la case **Enable DHCP**

Broadcast flag for DHCP request and discover messages (Activer l'indicateur de diffusion DHCP pour les demandes DHCP et les messages de découverte).

Le serveur DHCP écoute cet indicateur de diffusion et diffuse le paquet de réponse si l'indicateur est défini sur 1.

5. (Facultatif) Pour renouveler le bail locatif, cliquez sur **Renew DHCP Lease** (Renouveler le bail locatif DHCP).

Étape 7 (Facultatif) Dans le champ **Description**, saisissez une description pour le groupe de ponts.

Étape 8 Cliquez sur **OK**.

Une interface virtuelle de pont (BVI) est ajoutée au tableau d'interfaces, avec les interfaces physiques et sous-interfaces.

Configurer les paramètres généraux de l'interface de membre du groupe de ponts

Cette procédure décrit comment définir le nom, le niveau de sécurité et le groupe de ponts pour chaque interface membre du groupe de ponts.

Avant de commencer

- Un même groupe de ponts peut inclure différents types d'interfaces : des interfaces physiques, des sous-interfaces VLAN, des interfaces VNI et des EtherChannels. Le protocole PPPoE n'est pas pris en charge sur l'interface de gestion. En mode routé, les EtherChannels et les VNI ne sont pas pris en charge.
- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List, double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.
- Pour le mode transparent, n'utilisez pas cette procédure pour les interfaces de gestion; consultez Configurer une interface de gestion pour le mode transparent, à la page 705 pour configurer l'interface de gestion.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Les BVI apparaissent dans le tableau à côté des interfaces physiques, des sous-interfaceset des interfaces de canal de port EtherChannel. En mode de contexte multiple, seules les interfaces qui ont été affectées au contexte dans l'espace d'exécution du système apparaissent dans le tableau.

Étape 2 Choisissez la ligne correspondant à une interface non BVI, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche sous l'onglet **General** (Général).

Remarque Pour Firepower 1010, vous ne pouvez pas configurer de ports de commutation en tant que membres d'un groupe de ponts.

Vous ne pouvez pas mélanger des interfaces VLAN logiques et des interfaces de routeur physiques dans le même groupe de ponts.

Remarque En mode routé, les interfaces **port-channel** et **vni** ne sont pas prises en charge en tant que membres de groupes de ponts.

Étape 3 Dans le menu déroulant **Bridge Group** (Groupe de ponts), choisissez le groupe de ponts auquel vous souhaitez affecter cette interface.

Étape 4 Dans le champ **Interface Name** (Nom d'interface), saisissez un nom renfermant au maximum 48 caractères.

Étape 5 Dans le champ **Security level** (Niveau de sécurité), saisissez un niveau compris entre 0 (le plus bas) et 100 (le plus élevé).

Étape 6 Si l'interface n'est pas déjà activée, cochez la case **Enable Interface** (Activer l'interface).

Remarque Le champ **Channel Group** (Groupe de canaux) est en lecture seule et indique si l'interface fait partie d'un EtherChannel.

Étape 7 (Facultatif) Si vous installez un module et que vous souhaitez démontrer la fonctionnalité du module sur un ASA hors production, cochez la case **Forward traffic to the ASA module for inspection and reporting** (Transférer le trafic vers le module ASA pour inspection et génération de rapports). Consultez le chapitre du module ou le guide de démarrage rapide pour en savoir plus.

Étape 8 (Facultatif) Dans le champ **Description**, saisissez une description pour cette interface.

La description peut contenir jusqu'à 240 caractères sur une seule ligne (sans retour chariot). Dans le cas d'une liaison de basculement ou d'état, la description fixe est « LAN Failover Interface », « STATE Failover Interface » ou « LAN/STATE Failover Interface » par exemple. Vous ne pouvez pas modifier cette description. La description fixe remplace toute description que vous saisissez ici si vous faites de cette interface une liaison de basculement ou un lien d'état.

Étape 9 Cliquez sur **OK**.

Sujets connexes

Configurer l'adresse MAC manuelle, la MTU et le TCP MSS, à la page 737

Configurer une interface de gestion pour le mode transparent

En mode de pare-feu transparent, toutes les interfaces doivent appartenir à un groupe de ponts. La seule exception est l'interface de gestion (l'interface physique, une sous-interface (si prise en charge pour votre modèle) ou une interface EtherChannel composée d'interfaces de gestion (si vous avez plusieurs interfaces de gestion)) que vous pouvez configurer en tant qu'interface de gestion distincte; pour le Châssis

Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion que vous avez attribuée au périphérique logique ASA. Vous ne pouvez pas utiliser d'autres types d'interfaces comme interfaces de gestion. Vous pouvez configurer une interface de gestion en mode unique ou par contexte. Pour obtenir plus de renseignements, consultez Interface de gestion pour le mode transparent, à la page 613.

L'interface de gestion traite uniquement le trafic entrant et sortant et ne peut pas transmettre de trafic de transit.

Avant de commencer

- N'attribuez pas cette interface à un groupe de ponts; un groupe de ponts non configurable (ID 301) est automatiquement ajouté à votre configuration. Ce groupe de ponts n'est pas inclus dans la limite de groupes de ponts.
- Pour le Châssis Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion que vous avez attribuée au périphérique logique ASA.
- En mode de contexte multiple, vous ne pouvez partager aucune interface, y compris l'interface de gestion, entre les contextes. Vous devez vous connecter à une interface de données.
- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List (Liste des périphériques) et double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Choisissez la ligne correspondant à une interface de gestion, une sous-interface ou une interface de canal de port EtherChannel composée d'interfaces de gestion, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (modifier l'interface) s'affiche sous l'onglet **General** (général).

Pour le Châssis Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion (individuelle ou EtherChannel) que vous avez attribuée au périphérique logique ASA.

Étape 3 Dans le menu déroulant **Bridge Group** (Groupe de ponts), laissez la valeur par défaut **--None--** (--Aucune--). Vous ne pouvez pas attribuer une interface de gestion à un groupe de ponts.

Étape 4 Dans le champ **Interface Name** (Nom d'interface), saisissez un nom renfermant au maximum 48 caractères.

Étape 5 Dans le champ **Security level** (Niveau de sécurité), saisissez un niveau compris entre 0 (le plus bas) et 100 (le plus élevé).

Remarque La case **Dedicate this interface to management only** (Dédier cette interface à la gestion uniquement) est activée par défaut et n'est pas configurable.

Étape 6 Si l'interface n'est pas déjà activée, cochez la case **Enable Interface** (Activer l'interface).

Étape 7 Pour définir l'adresse IP, utilisez l'une des options suivantes.

Remarque Pour une utilisation avec le basculement, vous devez définir manuellement l'adresse IP et l'adresse en veille; le protocole DHCP n'est pas pris en charge. Définissez les adresses IP de veille dans l'onglet **Configuration > Device Management (Gestion des périphériques) > High Availability (Haute disponibilité) > Failover (Basculement) > Interfaces**.

- Pour définir l'adresse IP manuellement, cliquez sur le bouton radio **Use Static IP** (Utiliser l'adresse IP statique) et saisissez l'adresse IP et le masque.
- Pour obtenir une adresse IP d'un serveur DHCP, cliquez sur le bouton radio **Obtain Address via DHCP** (Obtenir l'adresse par DHCP).
  - Pour forcer le stockage d'une adresse MAC dans un paquet de demande DHCP pour l'option 61, cliquez sur le bouton radio **Use MAC Address** (Utiliser l'adresse MAC).

    Certains fournisseurs de services Internet s'attendent à ce que l'option 61 soit l'adresse MAC de l'interface. Si l'adresse MAC n'est pas incluse dans le paquet de demande DHCP, aucune adresse IP ne sera attribuée.
  - Pour utiliser une chaîne générée pour l'option 61, cliquez sur **Use "Cisco-<MAC>-<interface_name>-<host>"** (Utiliser « Cisco-<MAC>-<interface_name>-<host> »).
  - (Facultatif) Pour obtenir la route par défaut à partir du serveur DHCP, cochez **Obtain Default Route Using DHCP** (Obtenir la route par défaut en utilisant DHCP).
  - (Facultatif) Pour définir l'indicateur de diffusion sur 1 dans l'en-tête de paquet DHCP, lorsque le client DHCP envoie une découverte demandant une adresse IP, cochez la case **Enable DHCP Broadcast flag for DHCP request and discover messages** (Activer l'indicateur de diffusion DHCP pour les demandes DHCP et les messages de découverte).

    Le serveur DHCP écoute cet indicateur de diffusion et diffuse le paquet de réponse si l'indicateur est défini sur 1.
  - (Facultatif) Pour renouveler le bail locatif, cliquez sur **Renew DHCP Lease** (Renouveler le bail locatif DHCP).

Étape 8 (Facultatif) Dans le champ **Description**, saisissez une description pour cette interface.

La description peut contenir jusqu'à 240 caractères sur une seule ligne (sans retour chariot).

Étape 9 Cliquez sur **OK**.

Configuration de l'adressage IPv6

Cette section décrit comment configurer l'adressage IPv6.

À propos d'IPv6

Cette section comprend des informations sur IPv6.

Adresse IPv6

Vous pouvez configurer deux types d'adresses de monodiffusion pour IPv6 :

- Adresse globale (global) : l'adresse globale est une adresse publique que vous pouvez utiliser sur le réseau public. Pour un groupe de ponts, cette adresse doit être configurée pour les BVI, et non par interface membre. Vous pouvez également configurer une adresse IPv6 globale pour l'interface de gestion en mode transparent.
- Adresse locale du lien (link-local) : l'adresse locale du lien est une adresse privée que vous ne pouvez utiliser que sur le réseau directement connecté. Les routeurs ne transfèrent pas les paquets en utilisant des adresses locales du lien; ils sont uniquement destinés à la communication sur un segment de réseau physique donné. Ils peuvent être utilisés pour la configuration des adresses ou pour les fonctions de découverte du voisin telles que la résolution d'adresses. Dans un groupe de ponts, seules les interfaces membres ont des adresses de lien locales; les BVI n'ont pas d'adresse locale de lien.

Au minimum, vous devez configurer une adresse locale de lien pour que IPv6 fonctionne. Si vous configurez une adresse globale, une adresse locale de lien est automatiquement configurée sur l'interface, vous n'avez donc pas besoin de configurer spécifiquement une adresse locale de lien. Pour les interfaces membres des groupes de ponts, lorsque vous configurez l'adresse globale sur les BVI, ASA génère automatiquement des adresses link-local pour les interfaces membres. Si vous ne configurez pas d'adresse globale, vous devez configurer l'adresse locale de lien. La configuration peut s'effectuer automatiquement ou manuellement.

ID d'interface EUI-64 modifiée

RFC 3513 : IPv6 (Internet Protocol Version 6) exige que la partie identifiant d'interface de toutes les adresses IPv6 de monodiffusion, à l'exception de celles qui commencent par la valeur binaire 000, ait une longueur de 64 bits et soit bâtie au format EUI-64 modifié. L'ASA peut appliquer cette exigence pour les hôtes associés au lien local.

Lorsque cette fonctionnalité est activée sur une interface, les adresses source des paquets IPv6 reçus sur cette interface sont comparées aux adresses MAC sources pour s'assurer que les identifiants d'interface utilisent le format EUI-64 modifié. Si les paquets IPv6 n'utilisent pas le format EUI-64 modifié comme identifiant d'interface, les paquets sont abandonnés et le message de journal système suivant est généré :

```
325003: EUI-64 source address check failed.
```

La vérification du format de l'adresse n'est effectuée que lors de la création d'un flux. Les paquets d'un flux existant ne sont pas vérifiés. De plus, la vérification de l'adresse ne peut être effectuée que pour les hôtes du lien local.

Configurer le client de délégation de préfixe IPv6

L'ASA peut servir de client de délégation de préfixe DHPCv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que l'ASA peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes.

À propos de la délégation de préfixe IPv6

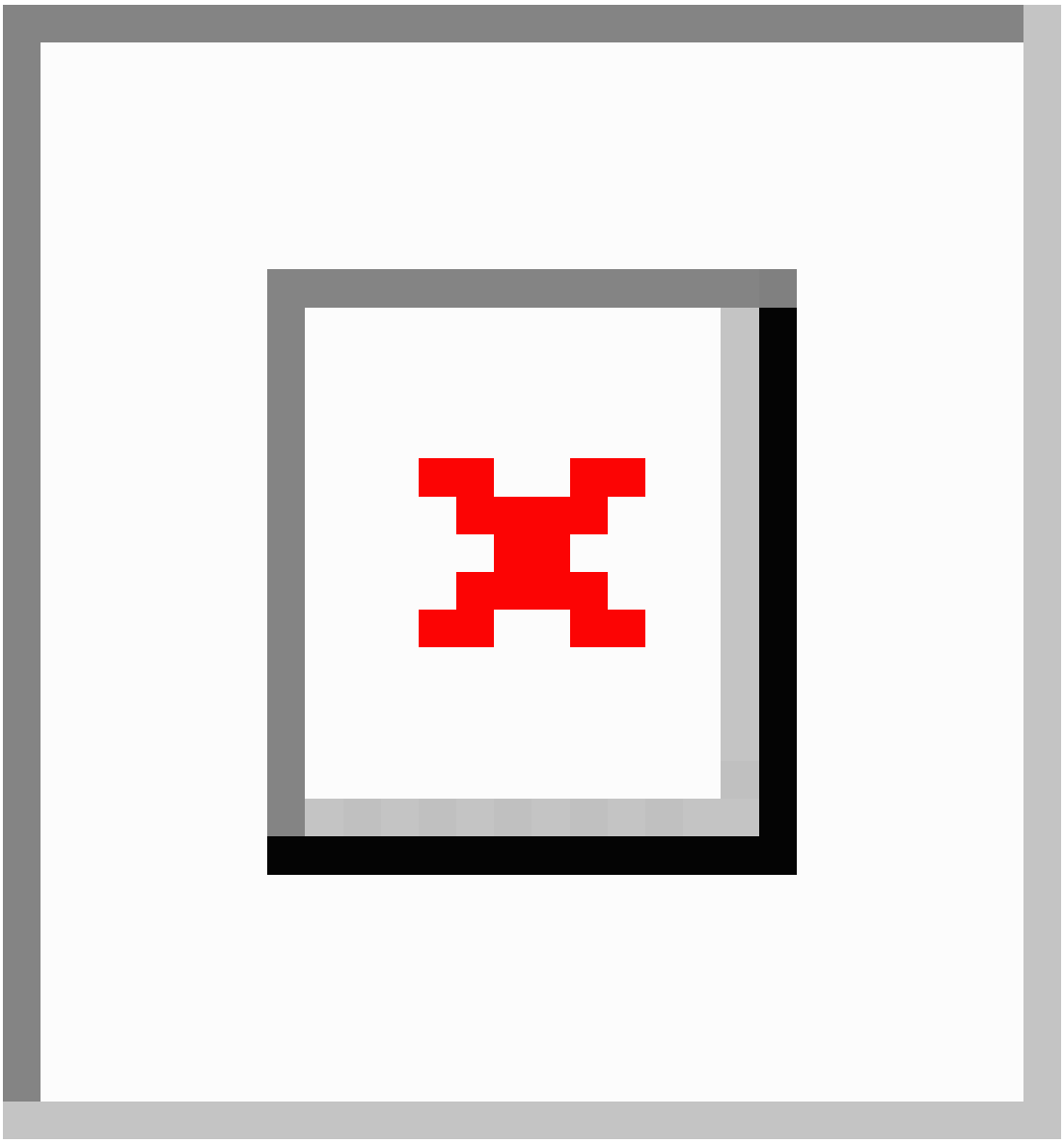
L'ASA peut servir de client de délégation de préfixe DHPCv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que l'ASA peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes. Les hôtes connectés aux interfaces internes

peuvent ensuite utiliser la configuration automatique sans état (SLAAC) pour obtenir des adresses IPv6 globales. Notez que les interfaces ASA internes n'agissent pas à leur tour comme des serveurs de délégation de préfixe; L'ASA ne peut fournir des adresses IP globales qu'aux clients SLAAC. Par exemple, si un routeur est connecté à l'ASA, il peut agir en tant que client SLAAC pour obtenir son adresse IP. Mais si vous souhaitez utiliser un sous-réseau du préfixe délégué pour les réseaux derrière le routeur, vous devez configurer manuellement ces adresses sur les interfaces internes du routeur.

L'ASA comprend un serveur DHCPv6 léger, de sorte que l'ASA peut fournir des informations telles que le serveur DNS et le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que ASA a reçu à l'aide de la délégation de préfixe.

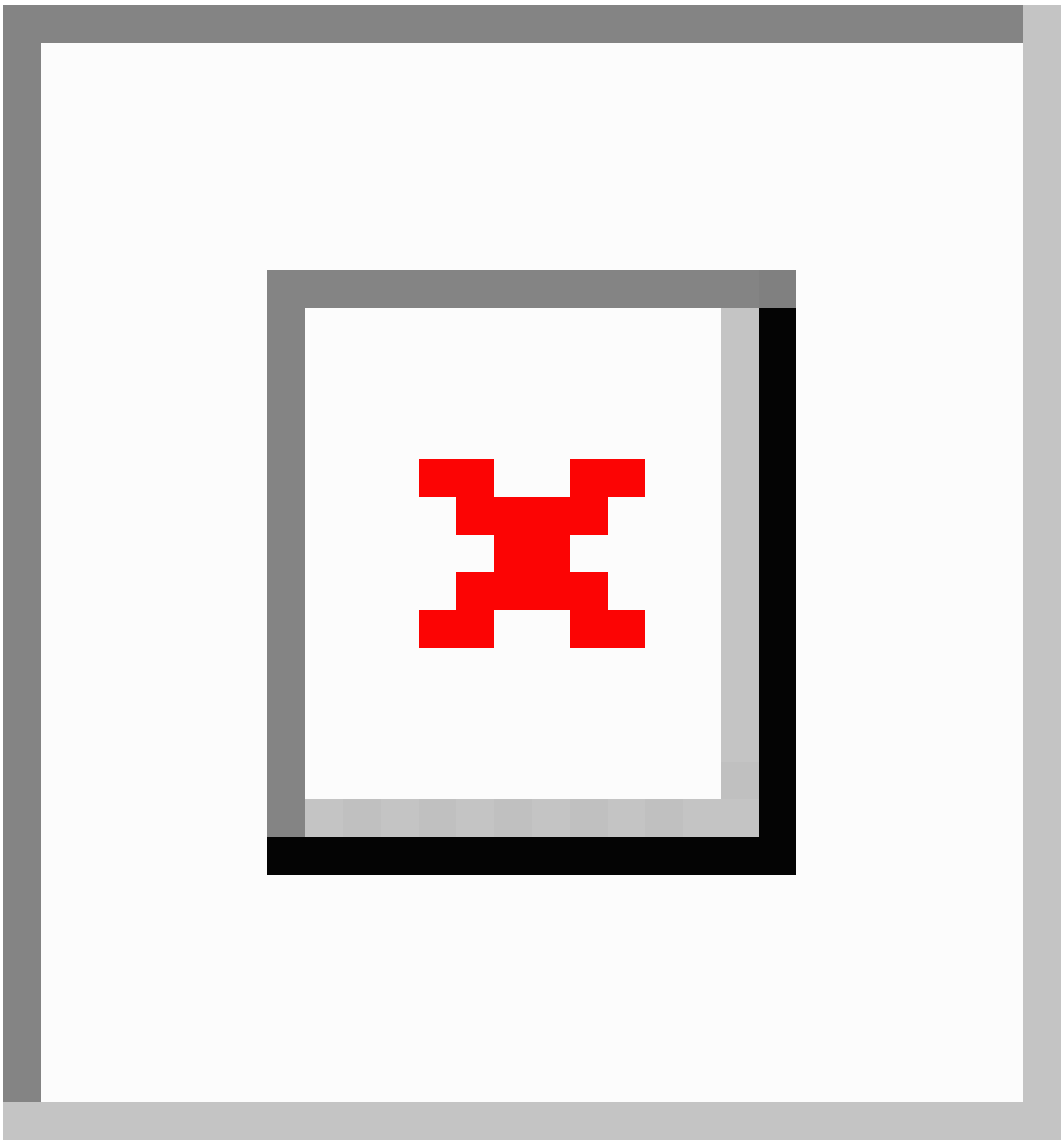
Exemple de délégation de préfixe IPv6 /de sous-réseau 64

L'exemple suivant montre que ASA reçoit une adresse IP sur l'interface externe en utilisant l'adresse DHCPv6. Il obtient également un préfixe délégué à l'aide du client de délégation de préfixe DHCPv6. L'ASA subdivise le préfixe délégué en réseaux /64 et attribue des adresses IPv6 globales à ses interfaces internes de manière dynamique en utilisant le préfixe délégué plus un sous-réseau configuré manuellement (::0, ::1 ou ::2) et une adresse IPv6 (0:0:0:1) par interface. Les clients SLAAC connectés à ces interfaces internes obtiennent des adresses IPv6 sur chaque sous-réseau /64.



Exemple de délégation de préfixe IPv6 /de sous-réseau 62

L’exemple suivant montre la sous-réseaux ASA du préfixe en 4 sous-réseaux /62 : 2001:DB8:ABCD:123**0**:/62, 2001:DB8:ABCD:123**4**:/62, 2001:DB8:ABCD:123**8**::/62 et 2001:DB8:ABCD:123 **C**::/62. ASA utilise l’un des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1230::/62 pour son réseau interne (::0). Vous pouvez ensuite utiliser manuellement des sous-réseaux /62 supplémentaires pour les routeurs en aval. Le routeur illustré utilise 3 des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1234::/62 pour ses interfaces internes (::4,::5 et::6). Dans ce cas, les interfaces de routeur internes ne peuvent pas obtenir dynamiquement le préfixe délégué. Vous devez donc afficher le préfixe délégué sur ASA, puis utiliser ce préfixe pour la configuration de votre routeur. Habituellement, les fournisseurs de services Internet délèguent le même préfixe à un client donné à l’expiration du bail, mais si ASA reçoit un nouveau préfixe, vous devrez modifier la configuration du routeur pour utiliser le nouveau préfixe. L'identifiant unique (DUID) de DHCP est persistant pendant les redémarrages.



Activer le client de délégation de préfixe IPv6

Activez le client de délégation de préfixe DHCPv6 sur une ou plusieurs interfaces. L'ASA obtient un ou plusieurs préfixes IPv6 qu'elle peut subdiviser en sous-réseaux et attribuer à des réseaux internes. En règle générale, l'interface sur laquelle vous activez la délégation de préfixe client obtient son adresse IP à l'aide de l'adresse client DHCPv6; Seules les autres interfaces ASA utilisent des adresses dérivées du préfixe délégué.

Avant de commencer

- Cette fonction n'est prise en charge qu'en mode pare-feu routé.
- Cette fonctionnalité n'est pas prise en charge en mode contexte multiple.
- Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe.
- Vous ne pouvez pas configurer cette fonction sur une interface de gestion uniquement.

- Lorsque vous utilisez la délégation de préfixe, vous devez définir l'intervalle d'annonce du routeur de découverte des voisins IPv6 de l'ASA de manière à ce qu'il soit bien inférieur à la durée de vie souhaitée du préfixe attribué par le serveur DHCPv6, afin d'éviter toute interruption du trafic IPv6. Par exemple, si le serveur DHCPv6 définit la durée de vie préférée de délégation de préfixe à 300 secondes, vous devez définir l'intervalle d'annonce de routeur de l'ASA à 150 secondes. Pour définir la durée de vie préférée, utilisez la commande **show ipv6 general-prefix**. Pour définir l'intervalle d'annonce de routeur de l'ASA, consultez Configurer la découverte des voisins IPv6, à la page 716; la valeur par défaut est de 200 secondes.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Choisissez une interface et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (modifier l'interface) s'affiche sous l'onglet **General** (général).

Étape 3 Cliquez sur l'onglet **IPv6**.

Étape 4 Dans a zone **Interface IPv6 DHCP** (Interface IPv6 DHCP), cliquez sur e bouton radio **Client Prefix Delegation Name** (Nom de la délégation du préfixe du client), et saisissez le nom du préfixe.

Étape 5 (Facultatif) Dans le champ **Prefix Hint** (conseils de préfixe), fournissez un ou plusieurs conseils sur le préfixe délégué que vous souhaitez recevoir.

Typiquement, vous voulez demander une longueur de préfixe particulière, comme ::/60, ou si vous avez déjà reçu un préfixe particulier et que vous voulez vous assurer de l'obtenir à nouveau à l'expiration du bail, vous pouvez saisir le préfixe entier comme indice (2001:DB8:ABCD:1230::/60). Si vous saisissez plusieurs conseils (préfixes ou longueurs différents), il appartient au serveur DHCP de choisir de respecter le conseil ou non.

Étape 6 Cliquez sur **OK**.

Vous retournez au volet **Configuration > Device Setup > Interface Settings > Interfaces** (Configuration > Configuration du périphérique > Paramètres d'interface > Interfaces).

Étape 7 Cliquez sur **Apply** (Appliquer).

Étape 8 Consultez Configuration d'une adresse globale IPv6, à la page 712 pour affecter un sous-réseau du préfixe comme adresse IP globale pour une interface ASA.

Étape 9 (Facultatif) Consultez Configurer le serveur sans état DHCPv6, à la page 789 pour fournir le nom de domaine et les paramètres de serveur aux clients SLAAC.

Étape 10 (Facultatif) Consultez Configurer les paramètres réseau IPv6, à la page 926 pour annoncer le ou les préfixes avec BGP.

Configuration d'une adresse globale IPv6

Pour configurer une adresse IPv6 globale pour une interface en mode routé et pour le BVI en mode transparent ou routé, procédez comme suit.

Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode de contexte multiple.

Remarque La configuration de l'adresse globale configure automatiquement l'adresse de lien local, de sorte que vous n'avez pas besoin de la configurer séparément. Pour les groupes de ponts, la configuration de l'adresse globale sur les BVI configure automatiquement les adresses de lien locales sur toutes les interfaces membres.

Pour les sous-interfaces, nous vous recommandons de définir également l'adresse MAC manuellement, car elles utilisent la même adresse MAC gravée de l'interface parente. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur l'ASA. Consultez Configurer l'adresse MAC manuelle, la MTU et le TCP MSS, à la page 737.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List (Liste des périphériques), double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Choisissez une interface et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (modifier l'interface) s'affiche sous l'onglet **General** (général).

En mode transparent ou pour un groupe de ponts en mode routé, sélectionnez un BVI. Pour le mode transparent, vous pouvez également sélectionner une interface de gestion uniquement.

Étape 3 Cliquez sur l'onglet **IPv6**.

Étape 4 Cochez la case **Enable IPv6** (activer IPv6).

Étape 5 (Facultatif) Pour appliquer l'utilisation des identifiants d'interface au format EUI-64 modifié dans les adresses IPv6 sur un lien local, cochez la case **Enforce EUI-64** (appliquer EUI-64).

Étape 6 (Interface routée) Configurez l'adresse IPv6 globale à l'aide de l'une des méthodes suivantes.

Pour le basculement et la mise en grappe, ainsi que pour les interfaces de boucle avec retour, vous devez définir l'adresse IP manuellement. Pour la mise en grappe, la configuration manuelle de l'adresse Link-Local n'est pas prise en charge.

- Autoconfiguration d'adresse sans état (SLAAC) : dans la zone **Interface IPv6 Addresses** (Adresses IPv6 de l'interface), cochez la case **Enable address autoconfiguration** (Activer l'autoconfiguration d'adresse).

  L'activation de la SLAAC sur l'interface configure les adresses IPv6 en fonction des préfixes reçus dans les messages d'annonce de routeur. Une adresse Link-Local, basée sur l'ID d'interface EUI-64 modifiée, est automatiquement générée pour l'interface lorsque la SLAAC est activée.

Remarque Bien que la RFC 4862 spécifie que les hôtes configurés pour une SLAAC n'envoient pas de messages d'annonce de routeur, l'ASA envoie ces messages dans ce cas. Cochez la case **Supprimer RA** pour supprimer les messages d'annonce.

Si vous souhaitez installer une route par défaut, choisissez **default trust dhcp** ou **default trust ignore** dans le menu déroulant. **default trust dhcp** spécifie que l'ASA utilise uniquement une route par défaut des annonces de routeurs provenant d'une source de confiance (c'est-à-dire du même serveur qui a fourni l'adresse IPv6). **default trust ignore** spécifie que les annonces de routeurs peuvent provenir d'un autre réseau, ce qui peut constituer une méthode plus risquée.

- Configuration manuelle : pour configurer manuellement une adresse IPv6 globale :

  1. Dans la zone **Interface IPv6 Addresses** (adresses IPv6 de l'interface), cliquez sur **Add** (Ajouter).

     La boîte de dialogue **Add IPv6 Address for Interface** (ajouter une adresse IPv6 pour l'interface) s'affiche.

  2. Dans le champ **Address/Prefix Longueur** (longueur d'adresse/préfixe), la valeur que vous saisissez dépend de la méthode que vous souhaitez utiliser :

     - Full global address (adresse globale complète) : si vous souhaitez saisir manuellement l'adresse complète, saisissez l'adresse complète plus la longueur du préfixe.
     - Modified EUI 64 format (format modifié EUI 64) : saisissez le préfixe et la longueur IPv6, puis cochez la case **EUI 64** pour générer l'ID d'interface en utilisant le format Modified EUI-64. Par exemple, 2001:0DB8::BA98:0:3210/48 (adresse complète) ou 2001:0DB8::/48 (préfixe, avec EUI 64 cochée).
     - Delegated Prefix (préfixe IPv6) : Pour dériver le préfixe IPv6 du préfixe délégué, saisissez l'adresse IPv6 et la longueur. Saisissez ensuite le nom de préfixe que vous avez configuré pour le client de délégation de préfixe DHCPv6 (voir Activer le client de délégation de préfixe IPv6, à la page 711) dans le champ **Prefix Name** (nom de préfixe), puis cliquez sur **Add** (Ajouter).

       En règle générale, le préfixe délégué est /60 ou moins, de sorte que vous pouvez créer un sous-réseau à plusieurs réseaux /64. /64 est la longueur de sous-réseau prise en charge si vous souhaitez prendre en charge SLAAC pour les clients connectés. Vous devez spécifier une adresse qui complète le sous-réseau /60, par exemple ::1:0:0:0:1. Saisissez : avant l'adresse si le préfixe est inférieur à 60. Par exemple, si le préfixe délégué est 2001:DB8:1234:5670::60, l'adresse IP globale attribuée à cette interface est 2001:DB8:1234:5671::1/64. Le préfixe annoncé dans les annonces des routeurs est 2001:DB8:1234:5671::/64. Dans cet exemple, si le préfixe est inférieur à 60, les bits restants du préfixe seront des 0, comme l'indique le préfixe::. Par exemple, si le préfixe est 2001:DB8:1234::/48, l'adresse IPv6 sera 2001:DB8:1234::1:0:0:0:1/64.

  3. Cliquez sur **OK**.

- Obtenez une adresse à l'aide de DHCPv6 :

  1. Dans la zone **Interface IPv6 DHCP**, cochez la case **Enable DHCP** (activer DHCP).
  2. (Facultatif) Cochez la case **Enable Default** (activer par défaut) pour obtenir une voie de routage par défaut à partir des annonces de routeur.

Étape 7 (interface BVI) Attribuez manuellement une adresse globale aux BVI. Pour une interface de gestion en mode transparent, utilisez également cette méthode.

a) Dans la zone **Interface IPv6 Addresses** (adresses IPv6 de l'interface), cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add IPv6 Address for Interface** (ajouter une adresse IPv6 pour l'interface) s'affiche.

b) Dans le champ **Address/Prefix Longueur** (longueur d'adresse/préfixe), saisissez l'adresse IPv6 globale complète ainsi que la longueur du préfixe IPv6.

c) Cliquez sur **OK**.

Étape 8 Cliquez sur **OK**.

Vous retournez au volet **Configuration > Device Setup > Interface Settings > Interfaces** (Configuration > Configuration du périphérique > Paramètres d'interface > Interfaces).

(Facultatif) Configurer automatiquement les adresses Link-Local

Si vous ne souhaitez pas configurer d'adresse globale et que vous avez seulement besoin de configurer une adresse Link-Local, vous avez la possibilité de générer les adresses Link-Local en fonction des adresses MAC de l'interface (format EUI-64 modifié. Comme les adresses MAC utilisent 48 bits, des bits supplémentaires doivent être insérés pour remplir les 64 bits requis pour l'ID d'interface.)

Pour configurer automatiquement les adresses Link-Local d'une interface, procédez comme suit.

Avant de commencer

Pris en charge en mode routé uniquement.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Sélectionnez une interface, puis cliquez sur **Edit**.

Pour les groupes de ponts en mode routé, choisissez la BVI.

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche sous l'onglet **General** (Général).

Étape 3 Cliquez sur l'onglet **IPv6**.

Étape 4 Dans la zone **IPv6 configuration** (Configuration IPv6), cochez la case **Enable IPv6** (Activer IPv6).

Cette option active IPv6 et génère automatiquement l'adresse Link-Local à l'aide de l'ID d'interface EUI-64 modifié en fonction de l'adresse MAC de l'interface.

Pour les groupes de ponts en mode routé, l'activation d'IPv6 pour la BVI génère des adresses Link-Local pour toutes les interfaces membres.

Étape 5 Cliquez sur **OK**.

(Facultatif) Configurer manuellement les adresses Link-Local

Si vous ne souhaitez pas configurer d'adresse globale et que vous avez seulement besoin de configurer une adresse link-local, vous avez la possibilité de définir manuellement cette dernière. Notez que nous vous recommandons d'attribuer automatiquement l'adresse de lien local en fonction du format EUI-64 modifié. Par exemple, si d'autres appareils imposent l'utilisation du format EUI-64 modifié, une adresse de lien local attribuée manuellement peut entraîner la perte de paquets.

Pour attribuer une adresse Link-Local à une interface, procédez comme suit.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Sélectionnez une interface, puis cliquez sur **Edit**.

Pour les groupes de ponts, choisissez une interface membre du groupe de ponts.

La boîte de dialogue **Edit Interface** (modifier l'interface) s'affiche sous l'onglet **General** (général).

Étape 3 Cliquez sur l'onglet **IPv6**.

Étape 4 (Facultatif) Pour appliquer l'utilisation des identifiants d'interface au format EUI-64 modifié dans les adresses IPv6 sur un lien local, cochez la case **Enforce EUI-64** (appliquer EUI-64).

Étape 5 Pour définir l'adresse Link-Local, saisissez une adresse dans le champ **Link-Local address** (Adresse Link-Local).

Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. Consultez Adresses IPv6, à la page 1355 pour en savoir plus sur l'adressage IPv6.

Étape 6 Cliquez sur **OK**.

Configurer la découverte des voisins IPv6

Le processus de découverte des voisins IPv6 utilise des messages ICMPv6 et des adresses de multidiffusion de nœud sollicité pour déterminer l'adresse de couche de liaison d'un voisin sur le même réseau (lien local), vérifier la lisibilité d'un voisin et suivre les routeurs voisins.

Les nœuds (hôtes) utilisent la découverte des voisins pour déterminer les adresses de couche de liaison des voisins connus pour résider sur les liens attachés et pour purger rapidement les valeurs en cache qui deviennent non valides. Les hôtes ont également recours à la découverte des voisins pour trouver les routeurs voisins qui sont prêts à transférer des paquets en leur nom. En outre, les nœuds utilisent le protocole pour garder activement une trace des voisins accessibles et de ceux qui ne le sont pas, et pour détecter les adresses de couche de liaison modifiées. Lorsqu'un routeur ou le chemin d'accès à un routeur tombe en panne, un hôte recherche activement des solutions de remplacement qui fonctionnent.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Choisissez l'interface IPv6 sur laquelle configurer les paramètres de voisin IPv6, puis cliquez sur **Edit** (Modifier).

Étape 3 Cliquez sur l'onglet **IPv6**.

Étape 4 Saisissez le nombre de **tentatives DAD**autorisées.

Les valeurs valides vont de 0 à 600. La valeur 0 désactive le traitement de la DAD sur l'interface spécifiée. La valeur par défaut est de 1 message par seconde.

DAD garantit l'unicité des nouvelles adresses IPv6 de monodiffusion avant qu'elles ne soient attribuées et veille à ce que les adresses IPv6 en double soient détectées dans le réseau selon les liaisons. L'ASA utilise les messages de sollicitation des voisins pour effectuer le DAD.

Lorsqu'une adresse en double est identifiée, l'état de l'adresse est défini à DUPLICATE, l'adresse n'est pas utilisée et le message d'erreur suivant est généré :

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

Si l'adresse en double est l'adresse link-local de l'interface, le traitement des paquets IPv6 est désactivé sur l'interface. Si l'adresse en double est une adresse globale, l'adresse n'est pas utilisée.

Étape 5 Saisissez l'**intervalle NS** en millisecondes pour définir l'intervalle entre les retransmissions de sollicitation des voisins IPv6.

Les valeurs valides pour l'argument de valeur sont comprises entre 1000 et 3600 000 millisecondes.

Les messages de sollicitation des voisins (ICMPv6 de type 135) sont envoyés sur la liaison locale par les nœuds qui tentent de découvrir les adresses de couche de liaison d'autres nœuds sur la liaison locale. Après avoir reçu un message de sollicitation de voisin, le nœud de destination répond en envoyant un message d'annonce de voisin (ICPMv6 type 136) sur la liaison locale.

Une fois que le nœud source a reçu l'annonce de voisin, le nœud source et le nœud de destination peuvent communiquer. Les messages de sollicitation de voisin sont également utilisés pour vérifier l'accessibilité d'un voisin après avoir identifié l'adresse de couche de liaison d'un voisin. Lorsqu'un nœud souhaite vérifier l'accessibilité d'un voisin, l'adresse de destination dans un message de sollicitation de voisin est l'adresse de monodiffusion du voisin.

Des messages d'annonce de voisin sont également envoyés en cas de changement dans l'adresse de couche de liaison d'un nœud sur une liaison locale.

Étape 6 Saisissez la **Durée d'accessibilité** en secondes pour définir combien de temps un nœud IPv6 distant est accessible.

Définissez la durée accessible entre 0 et 3600 000 millisecondes. Lorsque vous définissez la durée sur 0, la durée accessible est envoyée comme indéterminée. Il appartient aux périphériques de réception de définir et de suivre la durée accessible.

La durée d'accessibilité du voisin permet de détecter les voisins non disponibles. Des durées configurées plus courtes permettent de détecter plus rapidement les voisins non disponibles, mais des durées plus courtes consomment plus de bande passante réseau IPv6 et de ressources de traitement dans tous les périphériques réseau IPv6. Des durées configurées très courtes ne sont pas recommandées pour le fonctionnement normal d'un IPv6.

Étape 7 Saisissez la **durée de vie RA** en secondes pour définir la durée pendant laquelle les nœuds de la liaison locale considèrent l'ASA comme le routeur par défaut sur la liaison.

Les valeurs sont comprises entre 0 et 9 000 secondes. Si la valeur 0 est saisie, l'ASA ne doit pas être considéré comme un routeur par défaut sur l'interface sélectionnée.

Étape 8 Cochez la case **Suppress RA** (Supprimer les annonces de routeur) pour supprimer les annonces de routeur.

Les messages d'annonce de routeur (ICMPv6 Type 134) sont automatiquement envoyés en réponse aux messages de sollicitation de routeur (ICMPv6 Type 133). Les messages de sollicitation de routeur sont envoyés par les hôtes au démarrage du système, ce qui permet à l'hôte de se configurer automatiquement sans avoir à attendre le prochain message de publicité de routeur planifié.

Vous pouvez souhaiter désactiver ces messages sur toute interface pour laquelle vous ne souhaitez pas que l'ASA fournisse le préfixe IPv6 (par exemple, l'interface extérieure).

L'activation de cette option fait en sorte que l'ASA s'affiche comme un voisin IPv6 standard sur la liaison et non comme un routeur IPv6.

Étape 9 Saisissez l'**intervalle RA** pour définir l'intervalle entre les transmissions des annonces du routeur IPv6.

Les valeurs valides vont de 3 à 1 800 secondes. La valeur par défaut est de 200 secondes.

Pour ajouter une valeur d'intervalle de transmission d'annonce de routeur en millisecondes, cochez la case **RA Interval in Milliseconds** (Intervalle d'annonce de routeur en millisecondes) et saisissez une valeur comprise entre 500 et 1 800 000.

Pour empêcher la synchronisation avec d'autres nœuds IPv6, l'ASA ajuste de manière aléatoire la valeur que vous avez définie (gigue).

Étape 10 Cochez la case **Hosts should use DHCP for address config** (Les hôtes doivent utiliser DHCP pour la configuration des adresses) pour informer les clients d'autoconfiguration d'adresse sans état (SLAAC) IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des adresses, en plus de l'adresse d'autoconfiguration sans état dérivée.

Cette option définit l'indicateur de configuration d'adresse gérée dans le paquet d'annonce du routeur IPv6.

Étape 11 Cochez la case **Hosts should use DHCP for non-address config** (Les hôtes doivent utiliser DHCP pour la configuration sans adresses) pour informer les clients SLAAC IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des renseignements supplémentaires de DHCPv6, tels que l'adresse du serveur DNS.

Cette option définit l'indicateur Another Address Config (Configuration d'une autre adresse) dans le paquet d'annonce du routeur IPv6.

Étape 12 Configurez les préfixes IPv6 à inclure dans les annonces de routeur IPv6.

a) Dans la zone **Interface IPv6 Prefixes** (Préfixes IPv6 d'interface) , cliquez sur **Add** (Ajouter).
b) Saisissez la **longueur de l'adresse/du préfixe** ou cochez la case **par défaut** pour utiliser le préfixe par défaut.
c) Cochez la case **No Auto-Configuration** pour forcer les hôtes à configurer l'adresse IPv6 manuellement. Les hôtes de la liaison locale avec le préfixe précisé ne peuvent pas utiliser SLAAC IPv6.
d) Cochez la case **Aucune annonce** pour désactiver l'annonce de préfixe. Pour le préfixe **Default** (Par défaut), ce paramètre s'applique uniquement aux préfixes sur la liaison. Les préfixes hors liaison seront toujours annoncés, sauf si vous spécifiez **No Advertisements** (Aucune annonce) pour un préfixe hors liaison précis.
e) Cochez la case **Off Link** (hors-lien) pour configurer le préfixe spécifié comme hors lien. Le préfixe sera annoncé avec le bit L en effacement. Le préfixe ne sera pas inséré dans la table de routage en tant que préfixe connecté.
f) Dans la zone **Prefix Lifetime** (Durée de vie du préfixe), spécifiez une **durée de vie** ou une **date d'expiration** de la durée de vie .

À l'expiration de la durée de vie préférée, l'adresse passe à l'état obsolète. Lorsqu'une adresse est dans un état obsolète, son utilisation est déconseillée, mais pas formellement interdite. Après l'expiration de la durée de vie valide, l'adresse devient non valide et ne peut pas être utilisée. La durée de vie valide doit être supérieure ou égale à la durée de vie préférée.

- **Durée de vie** : les valeurs sont comprises entre 0 et 4294967295. La durée de vie valide par défaut est de 2592000 (30 jours). La durée de vie préférée par défaut est 604800 (7 jours). La valeur maximale représente l'éternité.
- **Lifetime Expiration Date**(date d'expiration de la durée de vie) : choisissez un mois et un jour valides dans les listes déroulantes, puis saisissez une heure au format hh:mm.

g) Cliquez sur**OK** pour sauvegarder vos paramètres.

Étape 13 Cliquez sur **OK**.

Étape 14 Configurer un voisin IPv6 statique.

Les directives et limites suivantes s'appliquent à la configuration d'un voisin IPv6 statique :

- Cette fonctionnalité est similaire à l'ajout d'une entrée ARP statique. Si une entrée pour l'adresse IPv6 précisée existe déjà dans le cache de découverte des voisins (apprise par le processus de découverte des voisins IPv6), elle est automatiquement convertie en entrée statique. Ces entrées sont stockées dans la configuration lorsque la commande copy est utilisée pour stocker la configuration.
- Les entrées statiques de la mémoire cache de découverte du voisin IPv6 ne sont pas modifiées par le processus de découverte du voisin.
- Les journaux système ICMP générés sont provoqués par une actualisation régulière des entrées IPv6 neighbor. La minuterie par défaut de l'ASA pour l'entrée du voisin IPv6 est de 30 secondes, donc l'ASA génère des paquets de découverte et de réponse des voisins ICMPv6 toutes les 30 secondes. Si l'ASA est dotée d'interfaces LAN et d'état de basculement configurées avec des adresses IPv6, toutes les 30 secondes, des paquets de réponse et de découverte de voisin ICMPv6 seront générés par les deux ASA pour les adresses IPv6 configurées et celles liées au lien local. En outre, chaque paquet génère plusieurs syslogs (connexion ICMP et création ou démontage de l'hôte local), de sorte qu'il peut sembler que des syslogs ICMP sont générés en permanence. L'heure d'actualisation de l'entrée du voisin IPV6 peut être configurée sur l'interface de données normale, mais pas sur l'interface de basculement. Cependant, l'impact sur le CPU pour ce trafic de découverte de voisin ICMP est minime.

Consultez aussi Afficher et effacer les voisins détectés dynamiquement, à la page 720.

a) Choisissez **Configuration** > **Device Management** (Gestion des périphériques) > **Advanced** (Avancé) > **IPv6 Neighbor Discovery Cache** (Cache de découverte de voisin IPv6).
b) Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add IPv6 Static Neighbor** (Ajouter un voisin statique IPv6) s'affiche.

c) Dans la liste déroulante **Interface Name** (Nom de l'interface), choisissez une interface à laquelle ajouter le voisin.
d) Dans le champ **IP Address** (adresse IP), saisissez l'adresse IPv6 qui correspond à l'adresse de liaison de données locale, ou cliquez sur les points de suspension (…) pour rechercher une adresse.
e) Dans le champ **MAC address** (adresse MAC), saisissez l'adresse MAC (matérielle) de la ligne de données locale.
f) Cliquez sur **OK**.

Étape 15 Cliquez sur **Apply** (Appliquer) pour enregistrer la configuration en cours d'exécution.

Afficher et effacer les voisins détectés dynamiquement

Lorsqu'un hôte ou un nœud communique avec un voisin, ce voisin est ajouté au cache de découverte de voisin. Le voisin est supprimé du cache lorsqu'il n'y a plus de communication avec lui.

Pour afficher les voisins détectés dynamiquement et effacer ces voisins du cache de découverte des voisins IPv6, procédez comme suit :

Procédure

Étape 1 Choisissez **Monitoring** > **Interfaces** > **IPv6 Neighbor Discovery Cache** (Surveillance > Interfaces > Cache de découverte du voisin IPv6).

Vous pouvez afficher tous les voisins statiques et dynamiques détectés dans le volet du cache de découverte des voisins IPv6.

Étape 2 Pour effacer du cache tous les voisins détectés dynamiquement, cliquez sur **Effacer les entrées des voisins dynamiques**.

Le voisin détecté dynamiquement est supprimé du cache.

Remarque Cette procédure efface uniquement les voisins découverts dynamiquement du cache; elle n'efface pas les voisins statiques.

Supervision des interfaces en mode routé et en mode transparent

Vous pouvez superviser les statistiques d'interface, l'état, PPPoE, etc.

Remarque Pour les modèles Firepower et Secure Firewall, certaines statistiques ne sont pas affichées à l'aide des commandes ASA. Vous devez consulter des statistiques d'interface plus détaillées à l'aide des commandes FXOS.

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

Pour Firepower 2100 en mode plateforme, consultez aussi les commandes FXOS connect local-mgmt suivantes :

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

Consultez le guide de dépannage FXOS pour plus d'informations.

Statistiques et informations sur l'interface

- **Monitoring (Supervision) > Interfaces > Interface Graphs (Graphiques d'interface)**

  Vous permet d'afficher les statistiques d'interface sous forme de graphique ou de tableau. Si une interface est partagée entre les contextes, l'ASA affiche uniquement les statistiques du contexte actuel. Le nombre de statistiques affichées pour une sous-interface est un sous-ensemble du nombre de statistiques affichées pour une interface physique.

- **Monitoring (Supervision) > Interfaces > Interface Graphs (Graphiques d'interface) > Graph/Table (Graphique/Tableau)**

  Affiche un graphique pour les statistiques sélectionnées. La fenêtre Graph (Graphique) peut afficher jusqu'à quatre graphiques et tableaux à la fois. Par défaut, le graphique ou le tableau affiche les statistiques en temps réel. Si vous activez les mesures de l'historique, vous pouvez afficher les statistiques des périodes passées.

Renseignements sur DHCP

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **DHCP Client Lease Information (Renseignements sur le bail locatif du client DHCP)**.

  Cet écran affiche les adresses IP configurées des clients DHCP.

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **IPV6 DHCP Client PD Statistics (Statistiques PD du client DHCP IPV6)**

  Cet écran affiche les statistiques du client de délégation de préfixe DHCPv6 et indique le résultat du nombre de messages envoyés et reçus.

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **IPV6 DHCP Client Statistics (Statistiques du client DHCP IPV6)**

Cet écran affiche les statistiques du client DHCPv6 et indique le résultat du nombre de messages envoyés et reçus.

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **IPV6 DHCP Interface Statistics (Statistiques d'interface DHCP IPV6)**

  Cet écran affiche les renseignements DHCPv6 pour toutes les interfaces. Si l'interface est configurée pour la configuration du serveur sans état DHCPv6 (voir Configurer le serveur sans état DHCPv6, à la page 789), cet écran répertorie l'ensemble DHCPv6 utilisé par le serveur. Si l'interface a une configuration de client d'adresse DHCPv6 ou de client de délégation de préfixe, cet écran affiche l'état de chaque client et les valeurs reçues du serveur. Cet écran affiche également les statistiques des messages pour le serveur ou le client DHCP.

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **IPV6 DHCP HA Statistics (Statistiques DHCP IPV6 à haute disponibilité)**

  Cet écran affiche les statistiques de transaction entre les unités de basculement, y compris le nombre de fois où les renseignements DUID ont été synchronisés entre les unités.

Suivi du routage statique

- **Monitoring (Supervision) > Interfaces > Interface connection (Connexion d'interface) > Track Status (État du suivi)**

  Affiche des renseignements sur l'objet suivi.

- **Monitoring (Supervision) > Interfaces > Interface connection (Connexion d'interface) > Monitoring Statistics (Statistiques de surveillance)**

  Affiche les statistiques relatives au processus de supervision des SLA.

PPPoE

- **Monitoring (Supervision) > Interfaces > PPPoE Client (Client PPPoE) > PPPoE Client Lease Information (Renseignements sur le bail locatif du client DHCP)**

  Affiche des renseignements sur les connexions PPPoE actuelles.

ACL dynamiques

Monitoring (Supervision) > Interfaces > Dynamic ACLs (ACL dynamiques)

Affiche un tableau des ACL dynamiques, qui sont fonctionnellement identiques aux ACL configurées par l'utilisateur, sauf qu'elles sont créées, activées et supprimées automatiquement par l'ASA. Ces ACL ne s'affichent pas dans la configuration et ne sont visibles que dans ce tableau. Elles sont identifiées par le mot clé « (dynamique) » dans l'en-tête de l'ACL.

Exemples d'interfaces en mode routé et en mode transparent

Exemple de mode transparent avec 2 groupes de ponts

L'exemple suivant de mode transparent comprend deux groupes de ponts de trois interfaces chacun, plus une interface de gestion uniquement :

```
interface gigabitethernet 0/0
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

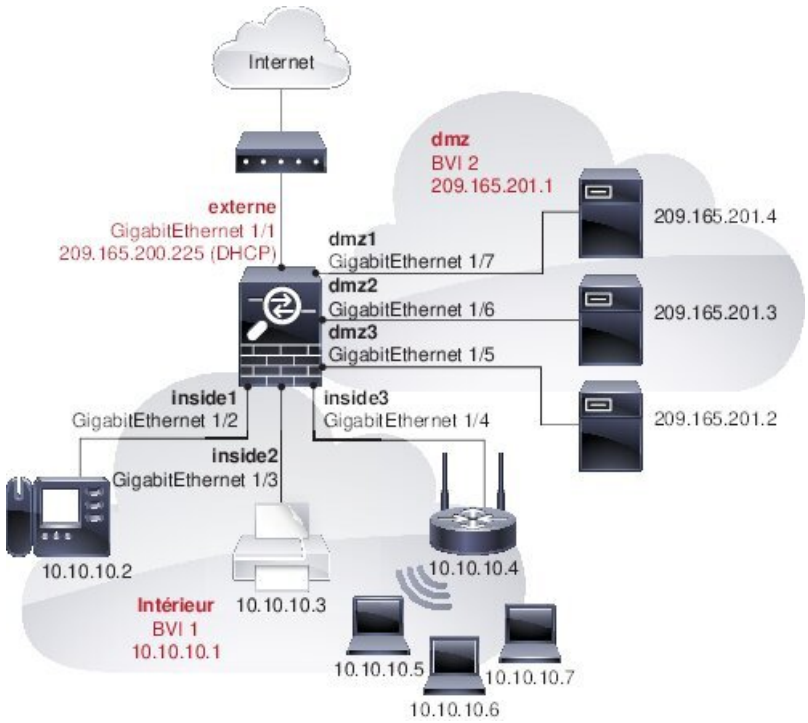
interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

Exemple de segment LAN commuté avec 2 groupes de ponts

Dans l'exemple suivant, deux groupes de ponts de 3 interfaces et une interface routée standard pour l'extérieur sont configurés. Le groupe de ponts 1 est à l'intérieur et le groupe de ponts 2 est une zone DMZ avec des serveurs Web publics. Les interfaces membres du groupe de ponts peuvent communiquer librement au sein du groupe de ponts, car chaque membre se trouve au même niveau de sécurité et nous avons activé la même

communication de sécurité. Bien que le niveau de sécurité du membre interne soit de 100 et que celui du membre de la zone DMZ soit également de 100, ces niveaux de sécurité ne s'appliquent pas aux communications inter-BVI; seuls les niveaux de sécurité BVI affectent le trafic inter-BVI. Les niveaux de sécurité des BVI et de l'extérieur (100, 50 et 0) autorisent implicitement le trafic de l'intérieur vers la zone DMZ et de l'intérieur vers l'extérieur; ainsi que de la zone DMZ vers l'extérieur. Un critère d'accès est appliqué à l'extérieur pour autoriser le trafic vers les serveurs de la zone DMZ.




```
interface gigabitethernet 1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface gigabitethernet 1/2
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/3
  nameif inside2
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/4
  nameif inside3
  security-level 100
  bridge-group 1
  no shutdown
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 10.10.10.1 255.255.255.0
```

```
!
interface gigabitethernet 1/5
  nameif dmz1
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/6
  nameif dmz2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/7
  nameif dmz3
  security-level 100
  bridge-group 2
  no shutdown
!
interface bvi 2
  nameif dmz
  security-level 50
  ip address 209.165.201.1 255.255.255.224
!
same-security-traffic permit inter-interface
!
# Assigns IP addresses to inside hosts
dhcpd address 10.10.10.2-10.10.10.200 inside
dhcpd enable inside
!
# Applies interface PAT for inside traffic going outside
nat (inside1,outside) source dynamic any interface
nat (inside2,outside) source dynamic any interface
nat (inside3,outside) source dynamic any interface
!
# Allows outside traffic to each server for specific applications
object network server1
  host 209.165.201.2
object network server2
  host 209.165.201.3
object network server3
  host 209.165.201.4
!
# Defines mail services allowed on server3
object-group service MAIL
  service-object tcp destination eq pop3
  service-object tcp destination eq imap4
  service-object tcp destination eq smtp
!
# Allows access from outside to servers on the DMZ
access-list SERVERS extended permit tcp any object server1 eq www
access-list SERVERS extended permit tcp any object server2 eq ftp
access-list SERVERS extended permit tcp any object server3 object-group MAIL
access-group SERVERS in interface outside
```

Historique des interfaces en mode routé et en mode transparent

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Découverte de voisin IPv6	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les écrans suivants : Monitoring (Supervision) > Interfaces > IPv6 Neighbor Discovery Cache (Cache de découverte de voisin IPv6). Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > IPv6 Neighbor Discovery Cache (Cache de découverte de voisin IPv6). Configuration > Device Setup (Gestion des périphériques) > Interface Settings (Paramètres d'interface) > Interfaces > IPv6.
Prise en charge d'IPv6 pour le mode transparent	8.2(1)	La prise en charge d'IPv6 a été introduite pour le mode de pare-feu transparent.
Groupes de ponts pour le mode transparent	v 8.4(1)	Si vous ne souhaitez pas le surdébit des contextes de sécurité ou si vous souhaitez optimiser votre utilisation des contextes de sécurité, vous pouvez regrouper les interfaces dans un groupe de ponts, puis configurer plusieurs groupes de ponts, un pour chaque réseau. Le trafic de groupe de ponts est isolé des autres groupes de ponts. Vous pouvez configurer jusqu'à huit groupes de ponts de quatre interfaces chacun en mode unique ou par contexte. Nous avons modifié ou introduit les écrans suivants : **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces** **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Bridge Group Interface (Ajouter/Modifier l'interface du groupe de ponts)** **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier l'interface)**
Indicateurs de configuration d'adresse pour le relais DHCP IPv6	9.0(1)	Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Interfaces > IPv6.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Nombre maximum de groupes de ponts en mode transparent augmenté à 250	9.3(1)	Le nombre maximum de groupes de ponts est passé de 8 à 250 groupes de ponts. Vous pouvez configurer jusqu'à 250 groupes de ponts en mode unique ou par contexte en mode multiple, avec 4 interfaces maximum par groupe de ponts. Nous avons modifié les écrans suivants : **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces** **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Bridge Group Interface (Ajouter/Modifier l'interface du groupe de ponts)** **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier l'interface)**
Nombre maximum d'interfaces en mode transparent par groupe de ponts augmenté à 64	9.6(2)	Le nombre maximum d'interfaces par groupe de ponts est passé de 4 à 64. Nous n'avons pas modifié d'écrans.
DHCP IPv6	9.6(2)	L'ASA prend désormais en charge les fonctionnalités suivantes pour l'adressage IPv6 : • Client d'adresse DHCPv6 : l'ASA obtient une adresse globale IPv6 et une route par défaut facultative du serveur DHCPv6. • Client de délégation de préfixe DHCPv6 : l'ASA obtient le ou les préfixes délégués d'un serveur DHCPv6. L'ASA peut ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface ASA afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. • Annonce de routeur BGP pour les préfixes délégués • Serveur sans état DHCPv6 : l'ASA fournit d'autres renseignements tels que le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresses aux clients. Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add Interface (Ajouter une interface)** > **IPv6** **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Pool (Réserve DHCP)** **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv6 Family (Famille IPv6)** > **Networks (Réseaux)** **Monitoring (Supervision)** > **Interfaces** > **DHCP**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage et pont intégrés	9.7(1)	Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que l'ASA relie par des ponts au lieu de routes. L'ASA n'est pas un vrai pont, car l'ASA continue d'agir comme un pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place. Auparavant, vous ne pouviez configurer les groupes de ponts qu'en mode de pare-feu transparent, où vous ne pouvez pas effectuer d'acheminement entre les groupes de ponts. Cette fonctionnalité vous permet de configurer des groupes de ponts en mode de pare-feu routé et pour effectuer le routage entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une solution de rechange au commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur l'ASA à affecter au groupe de ponts. En mode routé, les BVI peuvent être une interface nommée et participer séparément des interfaces membres à certaines fonctionnalités, telles que les règles d'accès et le serveur DHCP. Les fonctionnalités suivantes, prises en charge en mode transparent, ne sont pas prises en charge en mode routé : mode de contexte multiple, mise en grappe d'ASA. Les fonctionnalités suivantes ne sont pas prises en charge sur les BVI : le routage dynamique et le routage de multidiffusion. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Static Routes (Routes statiques)** **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Server (Serveur DHCP)** **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Critères d'accès)** **Configuration** > **Firewall (Pare-feu)** > **EtherType Rules (Règles EtherType)**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Masque de sous-réseau 31 bits	9.7(1)	Pour les interfaces routées, vous pouvez configurer une adresse IP sur un sous-réseau de 31 bits pour les connexions point à point. Le sous-réseau de 31 bits comprend seulement 2 adresses; normalement, la première et la dernière adresse du sous-réseau sont réservées pour le réseau et la diffusion, donc un sous-réseau à deux adresses n'est pas utilisable. Toutefois, si vous avez une connexion point à point et n'avez pas besoin d'adresses de réseau ou de diffusion, un sous-réseau de 31 bits est un moyen utile de conserver les adresses dans IPv4. Par exemple, la liaison de basculement entre 2 ASA ne nécessite que 2 adresses; les paquets transmis par une extrémité de la liaison sont toujours reçus par l'autre extrémité, et la diffusion n'est pas nécessaire. Vous pouvez également avoir une station de gestion directement connectée exécutant SNMP ou Syslog. Cette fonctionnalité n'est pas prise en charge pour les BVI pour les groupes de ponts ou avec le routage de multidiffusion. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add Interface (Ajouter une interface)** > **General (Général)**



CHAPITRE 22

Configuration avancée de l'interface

Ce chapitre décrit comment configurer les adresses MAC pour les interfaces, définir l'unité de transfert maximale (MTU), définir la taille de segment maximum TCP (TCP MSS) et autoriser une communication de même niveau de sécurité. La définition de la bonne MTU et de la taille de segment maximum TCP est essentielle pour garantir les meilleures performances du réseau.

- À propos des configurations avancées de l'interface, à la page 731
- Attribuer automatiquement des adresses MAC, à la page 736
- Configurer l'adresse MAC manuelle, la MTU et le TCP MSS, à la page 737
- Autoriser la communication de niveau de sécurité identique, à la page 738
- Supervision de l'ARP et du tableau d'adresses MAC, à la page 739
- Historique de la configuration avancée de l'interface, à la page 739

À propos des configurations avancées de l'interface

Cette section décrit les paramètres d'interface avancés.

À propos des adresses MAC

Vous pouvez affecter manuellement des adresses MAC pour remplacer la valeur par défaut. Pour le mode de contexte multiple, vous pouvez générer automatiquement des adresses MAC uniques (pour toutes les interfaces affectées à un contexte) et un mode de contexte unique (pour les sous-interfaces).

Remarque Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur ASA, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de liaison IPv6 sont générées sur la base de l'adresse MAC, l'attribution d'adresses MAC uniques aux sous-interfaces permet d'obtenir des adresses locales de liaison IPv6 uniques, ce qui peut éviter la perturbation du trafic dans certaines instances du périphérique ASA.

Adresses MAC par défaut

Les attributions d'adresses MAC par défaut dépendent du type d'interface.

- Interfaces physiques : l'interface physique utilise l'adresse MAC gravée.

- Interfaces VLAN (Firepower 1010) —Mode de pare-feu routé : toutes les interfaces VLAN partagent une adresse MAC. Assurez-vous que tous les commutateurs connectés peuvent prendre en charge ce scénario. Si les commutateurs connectés nécessitent des adresses MAC uniques, vous pouvez attribuer manuellement des adresses MAC. Consultez Configurer l'adresse MAC manuelle, la MTU et le TCP MSS, à la page 737

  Mode pare-feu transparent : chaque interface VLAN a une adresse MAC unique. Vous pouvez remplacer les adresses MAC générées si vous le souhaitez en attribuant manuellement des adresses MAC. Consultez Configurer l'adresse MAC manuelle, la MTU et le TCP MSS, à la page 737.

- EtherChannels : Pour un EtherChannel, toutes les interfaces du groupe de canaux partagent la même adresse MAC. Cette fonction rend l'EtherChannel transparent pour les applications et les utilisateurs du réseau, car ils ne voient qu'une seule connexion logique; ils n'ont aucune connaissance des liens individuels. L'interface du canal de port utilise une adresse MAC unique provenant d'un pool; L'appartenance à l'interface n'affecte pas l'adresse MAC.

- EtherChannels (modèles ASA) : l'interface du canal de port utilise l'adresse MAC d'interface de groupe de canaux du plus petit numéro comme adresse MAC du canal de port. Vous pouvez aussi configurer une adresse MAC pour l'interface du canal de port. Nous vous recommandons de configurer une adresse MAC unique au cas où l'appartenance à l'interface du canal de groupe changerait. Si vous supprimez l'interface qui fournissait l'adresse MAC du canal de port, l'adresse MAC du canal de port passe à l'interface ayant le numéro le plus bas, ce qui perturbe le trafic.

- Sous-interfaces : toutes les sous-interfaces d'une interface physique utilisent la même adresse MAC gravée. Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur ASA.

Adresses MAC automatiques

En mode de contexte multiple, la génération automatique affecte des adresses MAC uniques à toutes les interfaces affectées à un contexte.

Si vous attribuez manuellement une adresse MAC et activez la génération automatique, l'adresse MAC attribuée manuellement est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement est utilisée, si elle est activée.

Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC pour l'interface.

Comme les adresses générées automatiquement (lors de l'utilisation d'un préfixe) commencent par A2, vous ne pouvez pas commencer les adresses MAC manuelles par A2 si vous souhaitez également utiliser la génération automatique.

Le châssis génère l'adresse MAC en utilisant le format suivant :

A2*xx.yyzz.zzzz*

Où *xx.yy* est un préfixe défini par l'utilisateur ou un préfixe généré automatiquement en fonction des deux derniers octets de l'adresse MAC de l'interface, et *zz.zzzz* est un compteur interne généré par l'ASA. Pour l'adresse MAC de secours, l'adresse est identique, sauf que le compteur interne est augmenté de 1.

Pour donner un exemple d'utilisation du préfixe, si vous définissez le préfixe 77, l'ASA convertit 77 en valeur hexadécimale 004D (*yyxx*). Lorsqu'il est utilisé dans l'adresse MAC, le préfixe est inversé (*xxyy*) pour correspondre à la forme native de l'ASA :

A2**4D.00***zz.zzzz*

Pour un préfixe 1009 (03F1), l'adresse MAC est :

A2**F1.03***zz.zzzz*

Remarque Le format d'adresse MAC sans préfixe est une version existante. Consultez la commande **mac-address auto** dans la référence de commandes pour plus d'informations sur le format existant.

À propos de la MTU

La MTU spécifie la taille maximale de la *charge utile* de trame que l'ASA peut transmettre sur une interface Ethernet donnée. La valeur MTU correspond à la taille de la trame *sans* en-tête Ethernet, sans balisage VLAN ou autre surdébit. Par exemple, lorsque vous définissez la MTU sur 1500, la taille de trame attendue est de 1518 octets, en-têtes compris, ou de 1522 lorsque vous utilisez le VLAN. Ne définissez pas la valeur MTU plus élevée pour prendre en charge ces en-têtes.

Pour VXLAN ou Geneve, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet IP est plus volumineux et nécessite une MTU plus grande : vous devez définir la MTU de l'interface source VTEP ASA sur la MTU du réseau + 54 octets (pour VXLAN) ou + 306 octets (Geneve).

Chemin de découverte de MTU

L'ASA prend en charge la découverte de chemin MTU (comme défini dans la RFC 1191), qui permet à tous les périphériques d'un chemin réseau entre deux hôtes de coordonner la MTU afin qu'ils puissent normaliser sur la MTU la plus basse du chemin.

MTU par défaut

Par défaut, la MTU sur ASA est de 1500 octets. Cette valeur n'inclut pas les 18 à 22octets pour l'en-tête Ethernet, le balisage VLAN ou d'autres surdébits.

Lorsque vous activez VXLAN sur l'interface source VTEP, si la MTU est inférieure à 1 554 octets, l'ASA l'augmente automatiquement à 1 554 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. En général, vous devez définir la MTU de l'interface source de l'ASA comme étant la MTU du réseau + 54 octets.

MTU et fragmentation.

Pour IPv4, si un paquet IP sortant dépasse la MTU spécifiée, il est fragmenté en au moins deux trames. Les fragments sont réassemblés à la destination (et parfois aux sauts intermédiaires), et la fragmentation peut dégrader les performances. Pour IPv6, la fragmentation des paquets n'est généralement pas autorisée. Par conséquent, vos paquets IP doivent respecter la taille de la MTU pour éviter la fragmentation.

Pour les paquets TCP, les points terminaux utilisent généralement leur MTU pour déterminer la taille maximale du segment TCP (MTU – 40, par exemple). Si des en-têtes TCP supplémentaires sont ajoutés en cours de route, par exemple pour les tunnels VPN de site à site, le MSS TCP devra peut-être être ajusté par l'entité de tunnellisation. Consultez À propos de TCP MSS, à la page 734.

Pour UDP ou ICMP, l'application doit prendre en compte la MTU pour éviter la fragmentation.

Remarque L'ASA peut recevoir des trames plus grandes que la MTU configurée tant qu'il y a de l'espace en mémoire.

MTU et trames grand format

Une MTU plus grande vous permet d'envoyer des paquets plus volumineux. Des paquets plus volumineux pourraient être plus efficaces pour votre réseau. Consultez les consignes suivantes :

- Correspondance des MTU sur le chemin de trafic : nous vous recommandons de définir la MTU sur toutes les interfaces ASA et les autres interfaces de périphériques le long du chemin de trafic. La correspondance des MTU empêche les périphériques intermédiaires de fragmenter les paquets.
- Prise en charge des trames étendues : vous pouvez définir la MTU à 9 000 octets ou plus lorsque vous activez les trames étendues. Le maximum dépend du modèle.

À propos de TCP MSS

La taille maximale de segment (MSS) TCP est la taille de la charge utile TCP *avant* l'ajout des en-têtes TCP et IP. Les paquets UDP ne sont pas concernés. Le client et le serveur échangent des valeurs TCP MSS lors de la prise de contact tridirectionnelle lors de l'établissement de la connexion.

Vous pouvez définir le MSS TCP sur l'ASA pour le trafic de transit; par défaut, le MSS TCP maximal est défini sur 1380 octets. Ce paramètre est utile lorsque ASA doit augmenter la taille du paquet pour l'encapsulation VPN IPsec. Cependant, pour les points terminaux non IPsec, vous devez désactiver le MSS TCP maximal sur ASA.

Si vous définissez un MSS TCP maximal, si l'une ou l'autre des extrémités d'une connexion demande un MSS TCP supérieur à la valeur définie sur l'ASA, alors l'ASA remplace le MSS TCP dans le paquet de demande par l'ASA maximum. Si l'hôte ou le serveur ne demande pas de message MSS du protocole TCP, ASA assume la valeur par défaut de la RFC 793 de 536 octets (IPv4) ou de 1 220 octets (IPv6), mais ne modifie pas le paquet. Par exemple, vous laissez la MTU par défaut à 1500 octets. Un hôte demande un MSS de 1500 moins la longueur de l'en-tête TCP et IP, ce qui définit le MSS à 1460. Si le MSS TCP maximal de l'ASA est de 1 380 (par défaut), l'ASA modifie la valeur du MSS dans le paquet de demande TCP à 1380. Le serveur envoie ensuite des paquets avec une charge utile de 1380 octets. L'ASA peut alors ajouter jusqu'à 120 octets d'en-tête au paquet tout en conservant la taille de MTU de 1500.

Vous pouvez également configurer le MSS TCP minimal; si un hôte ou un serveur demande un très petit MSS TCP, ASA peut augmenter la valeur. Par défaut, le MSS TCP minimal n'est pas activé.

Pour le trafic vers la boîte, y compris pour les connexions SSL VPN, ce paramètre ne s'applique pas. L'ASA utilise la MTU pour calculer le TCP MSS : MTU – 40 (IPv4) ou MTU – 60 (IPv6).

TCP MSS par défaut

Par défaut, le MSS TCP maximal sur l'ASA est de 1380 octets. Cette valeur par défaut convient aux connexions VPN IPsec IPv4 où la valeur des en-têtes peut atteindre 120 octets; Cette valeur correspond à la MTU par défaut de 1500 octets.

Paramètre MSS TCP maximal suggéré

Le MSS TCP par défaut suppose que l'ASA agit comme un point terminal de VPN IPsec IPv4 et a une MTU de 1500. Lorsque l'ASA agit comme un point terminal de VPN IPsec IPv4, il doit gérer jusqu'à 120 octets pour les en-têtes TCP et IP.

Si vous modifiez la valeur MTU, utilisez IPv6 ou n'utilisez pas ASA comme point terminal VPN IPsec, vous devez modifier le paramètre TCP MSS.

Consultez les consignes suivantes :

- Normal Traffic (Trafic normal) : Désactivez la limite TCP MSS et acceptez la valeur établie entre les points terminaux de connexion. Étant donné que les points terminaux de connexion dérivent généralement le MSS TCP de la MTU, les paquets non IPsec correspondent généralement à ce MSS TCP.
- IPv4 IPsec endpoint traffic : Définissez le MSS TCP maximal sur la MTU - 120. Par exemple, si vous utilisez des trames étendues et que vous définissez la MTU à 9000, vous devez définir le MSS TCP sur 8880 pour profiter de la nouvelle MTU.
- IPv6 IPsec endpoint Traffic (Trafic de point terminal IPsec IPv6) : définissez le MSS TCP maximal sur la MTU - 140.

Communication inter-interface

Permettre à des interfaces de même niveau de sécurité de communiquer entre elles offre les avantages suivants :

- Vous pouvez configurer plus de 101 interfaces de communication.

  Si vous utilisez différents niveaux pour chaque interface et n'affectez aucune interface au même niveau de sécurité, vous ne pouvez configurer qu'une seule interface par niveau (de 0 à 100).
- Vous souhaitez que le trafic passe librement entre toutes les mêmes interfaces de sécurité sans ACL.

Si vous activez la même communication d'interface de sécurité, vous pouvez toujours configurer des interfaces à différents niveaux de sécurité, comme d'habitude.

Communication intra-interface (mode de pare-feu routé)

La communication intra-interface peut être utile pour le trafic VPN qui entre dans une interface, mais qui est ensuite acheminé vers la même interface. Dans ce cas, le trafic VPN peut être non chiffré ou rechiffré pour une autre connexion VPN. Par exemple, si vous avez un réseau VPN en étoile, où l'ASA est le concentrateur et les réseaux VPN distants sont des rayons, pour qu'un rayon communique avec un autre rayon, le trafic doit entrer dans l'ASA, puis ressortir vers l'autre rayon.



Remarque Tout le trafic autorisé par cette fonctionnalité reste soumis aux règles du pare-feu. Veillez à ne pas créer de situation de routage asymétrique qui pourrait empêcher le trafic de retour de traverser l'ASA.

Attribuer automatiquement des adresses MAC

Cette section décrit comment configurer la génération automatique des adresses MAC. Pour le mode de contexte multiple, cette fonctionnalité attribue des adresses MAC uniques à tous les types d'interfaces qui sont affectés à un contexte. Pour le mode de contexte unique, cette fonctionnalité attribue des adresses MAC uniques aux sous-interfaces VLAN.

Avant de commencer

- Lorsque vous configurez une nom pour l'interface, la nouvelle adresse MAC est générée immédiatement. Si vous activez cette fonctionnalité après avoir configuré les interfaces, les adresses MAC sont générées pour toutes les interfaces immédiatement après leur activation. Si vous désactivez cette fonctionnalité, l'adresse MAC par défaut de chaque interface revient à l'adresse MAC. Par exemple, les sous-interfaces de GigabitEthernet 0/1 utilisent l'adresse MAC de GigabitEthernet 0/1.
- Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC pour l'interface.
- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, dans le volet **Configuration** > **Device List (Liste des périphériques)**, double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Pour le mode de contexte multiple : effectuez les étapes suivantes dans le système.

a) Choisissez **Configuration** > **Context Management (Gestion des contextes)** > **Security Contexts (Contextes de sécurité)**.
b) Cochez **Mac-Address auto** (Adresse MAC auto).
c) (Facultatif) Cochez la case **Prefix** (Préfixe) et dans le champ, saisissez une valeur décimale entre 0 et 65 535.

   Ce préfixe est converti en nombre hexadécimal à quatre chiffres et utilisé dans l'adresse MAC. Si vous n'écrivez pas de préfixe, l'ASA génère automatiquement ce dernier en fonction des deux derniers octets de l'adresse MAC de l'interface.

Étape 2 Pour le mode de contexte unique : effectuez les étapes suivantes.

a) Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.
b) Au bas de la page, cochez la case **Enable auto-generation of MAC addresses for subinterfaces** (Activer la génération automatique des adresses MAC pour les sous-interfaces).
c) (Facultatif) Dans le champ **Prefix** (Préfixe), saisissez une valeur décimale entre 0 et 65 535.

   Ce préfixe est converti en nombre hexadécimal à quatre chiffres et utilisé dans l'adresse MAC. Si vous n'écrivez pas de préfixe, l'ASA génère automatiquement ce dernier en fonction des deux derniers octets de l'adresse MAC de l'interface.

Étape 3 Cliquez sur **Apply** (Appliquer).

Configurer l'adresse MAC manuelle, la MTU et le TCP MSS

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List, double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Choisissez la ligne d'interface, puis cliquez sur modifier (**Edit**).

La boîte de dialogue **Edit Interface** (modifier l'interface) s'affiche sous l'onglet **General** (général).

Étape 3 Cliquez sur l'onglet **Advanced (Avancé)**.

Étape 4 Pour définir le MTU ou activer la prise en charge des bâtis grand format (modèles pris en charge uniquement), saisissez la valeur dans le champ **MTU**. Le minimum et le maximum dépendent de votre plateforme.

Par défaut, la MTU est de 1500 octets.

Remarque Lorsque vous définissez le MTU pour une interface ou de canal de port, l'ASA applique le paramètre à toutes les interfaces membres.

- Pour les modèles qui prennent en charge les trames étendues dans le mode unique, si vous entrez une valeur pour une interface supérieure à 1500, vous devez activer la prise en charge de trame étendue automatique pour toutes les interfaces. Si vous réglez la MTU pour toutes les interfaces sur une valeur inférieure à 1500, la prise en charge des trames étendues est désactivée.
- Pour les modèles qui prennent en charge les bâtis grand format en mode multiple – Si vous entrez une valeur supérieure à 1500 pour une interface, assurez-vous d'activer la prise en charge des bâtis grand format dans la configuration système, si cela est nécessaire pour votre modèle. Consultez Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000), à la page 618.

Remarque Pour certains modèles, l'activation ou la désactivation de la prise en charge des bâtis grand format nécessite le rechargement de l'ASA.

Étape 5 Pour affecter manuellement une adresse MAC à cette interface, dans le champ **Active Mac Address** , entrez une adresse MAC au format H.H.H., où H est une valeur hexadécimale de 16 bits.

Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE serait saisie comme suit : 000C.F142.4CDE. Les deux premiers octets d'une adresse MAC manuelle ne peuvent pas être A2 si vous souhaitez également utiliser des adresses MAC générées automatiquement.

Étape 6 Si vous utilisez le basculement, entrez l'adresse MAC en veille dans le champ **Standby Mac Address**. Si l'unité active bascule et que l'unité en veille devient active, la nouvelle unité active commence à utiliser les adresses MAC actives pour minimiser les perturbations du réseau, tandis que l'ancienne unité active utilise l'adresse en veille.

Étape 7 Pour définir le MSS TCP, sélectionnez **Configuration** > **Firewall** > **Advanced** > **TCP Options**. Définissez les options suivantes :

- Envoyer la réponse de réinitialisation pour les paquets TCP externes refusés : Permet à l'ASA d'envoyer des réponses de réinitialisation pour toutes les sessions TCP sortantes qui tentent de transiter par l'ASA et qui sont refusées par l'ASA en fonction des listes d'accès ou des paramètres AAA.
- Force Maximum Segment Size for TCP (forcer la taille de segment maximal pour TCP) : Définissez la taille de segment TCP maximale en octets, entre 48 et tout nombre maximal. Par défaut, la MTU est de 1380 octets. Vous pouvez désactiver cette fonctionnalité en mettant les octets à 0.
- Force Minimum Segment Size for TCP (forcer la taille de segment minimal pour TCP) : Permet de remplacer la taille maximale du segment par le nombre d'octets que vous avez défini, entre 48 et tout nombre maximal. Cette fonctionnalité est désactivée par défaut (définie sur 0).

Étape 8 Pour les paramètres de balisage de groupe sécurisé (**Secure Group Tagging**), consultez le guide de configuration du pare-feu.

Étape 9 (Secure Firewall 3100) Cliquez sur **Auto-negotiate (négociation automatique)** pour négocier l'état de la liaison et le contrôle de flux pour les interfaces de 1 Gigabit et plus.

La négociation automatique est définie indépendamment de la vitesse. Certains commutateurs ne prennent pas en charge la négociation automatique, en particulier pour les interfaces à vitesse élevée. Dans ce cas, réglez l'interface ASA à une vitesse manuelle et désactivez également **Auto-negotiate** (Négociation automatique) afin que la liaison puisse s'établir.

Étape 10 Pour les paramètres de grappe d'ASA (**ASA Cluster**), consultez (Recommandé; requis en mode de contexte multiple) Configurer les interfaces sur le nœud de contrôle, à la page 387.

Autoriser la communication de niveau de sécurité identique

Par défaut, les interfaces de même niveau de sécurité ne peuvent pas communiquer entre elles, et les paquets ne peuvent pas entrer ni sortir de la même interface. Cette section décrit comment activer la communication inter-interfaces lorsque les interfaces se trouvent sur le même niveau de sécurité et comment activer la communication intra-interface.

Procédure

Étape 1 Pour permettre aux interfaces de même niveau de sécurité de communiquer entre elles, dans le volet **Configuration** > **Interfaces**, cochez la case **Enable traffic between two or more interfaces which are configured with same security level** (Activer le trafic entre deux ou plusieurs interfaces qui sont configurées avec le même niveau de sécurité).

Étape 2 Pour activer la communication entre les hôtes connectés à la même interface, cochez la case **Enable traffic between two or more hosts connected to the same interface** (Activer le trafic entre deux ou plusieurs hôtes connectés à la même interface).

Supervision de l'ARP et du tableau d'adresses MAC

- **Monitoring (Supervision) > Interfaces > ARP Table (Tableau ARP)**

  Affiche le tableau ARP, y compris les entrées statiques et dynamiques. Le tableau ARP comprend des entrées qui mappent une adresse MAC à une adresse IP pour une interface donnée.

- **Monitoring (Supervision) > Interfaces > MAC Address Table (Tableau d'adresses MAC)**

  Affiche les entrées d'adresse MAC statiques et dynamiques.

Historique de la configuration avancée de l'interface

Tableau 33 : Historique de la configuration avancée de l'interface

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
La MTU maximale est maintenant de 9 198 octets.	9.1(6), 9.2(1)	La MTU maximale que l'ASA peut utiliser est de 9 198 octets (vérifiez la limite exacte de votre modèle à l'aide de l'interface de ligne de commande). Cette valeur n'inclut pas l'en-tête de couche 2. L'ASA vous a permis de définir une MTU maximale de 65 535 octets, ce qui était inexact et pourrait causer des problèmes. Si votre MTU a été définie à une valeur supérieure à 9 198, la MTU est automatiquement réduite lors de la mise à niveau. Dans certains cas, cette modification de la MTU peut entraîner une non-concordance de la MTU. Assurez-vous de configurer tout équipement de connexion pour utiliser la nouvelle valeur MTU. Nous avons modifié l'écran suivant : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Edit Interface (Modifier l'interface)** > **Advanced (Avancé)**
Augmentation de la taille de la MTU pour l'ASA sur le Châssis Firepower 4100/9300	9.6(2)	Vous pouvez définir la MTU maximale à 9 184 octets sur les périphériques Firepower 4100 et 9300; auparavant, le maximum était de 9 000 octets. Cette MTU est prise en charge par FXOS 2.0.1.68 et les versions ultérieures. Nous avons modifié l'écran suivant : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Advanced (Avancé)**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Génération d'adresses MAC uniques en mode de contexte unique	9.8(3), 9.8(4), 9.9(2)	Vous pouvez maintenant activer la génération d'adresses MAC uniques pour les sous-interfaces VLAN en mode de contexte unique. Normalement, les sous-interfaces partagent la même adresse MAC avec l'interface principale. Comme les adresses Link-Local IPv6 sont générées en fonction de l'adresse MAC, cette fonctionnalité permet d'utiliser des adresses Link-Local IPv6 uniques. Commande nouvelle ou modifiée : **mac-address auto** ASDM n'est pas pris en charge.
Prise en charge d'ASDM pour la génération d'adresses MAC uniques en mode de contexte unique	ASDM 7.15(1)	Vous pouvez maintenant activer la génération d'adresses MAC uniques pour les sous-interfaces VLAN en mode de contexte unique dans ASDM. Normalement, les sous-interfaces partagent la même adresse MAC avec l'interface principale. Comme les adresses Link-Local IPv6 sont générées en fonction de l'adresse MAC, cette fonctionnalité permet d'utiliser des adresses Link-Local IPv6 uniques. Écran nouveau ou modifié : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**
La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée pour les interfaces de 1 Gigabit et les versions ultérieures.	9.17(1)	La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée pour les interfaces de 1 Gigabit et les versions ultérieures. Pour les autres modèles de ports SFP, l'option **no speed nonegotiate** définit la vitesse à 1 000 Mbit/s; la nouvelle commande signifie que vous pouvez définir la négociation automatique et la vitesse indépendamment. Écrans Nouveaux ou modifiés : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Advanced (Avancé)**



CHAPITRE 23

Zones de circulation

Vous pouvez attribuer plusieurs interfaces à une *zone de trafic*, ce qui permet au trafic d'un flux existant de sortir ou d'entrer dans l'ASA sur n'importe quelle interface de la zone. Cette fonctionnalité permet le routage à chemins multiples à coûts égaux (ECMP) sur l'ASA, ainsi qu'à équilibrer la charge externe du trafic vers l'ASA sur plusieurs interfaces.

- À propos des zones de trafic, à la page 741
- Conditions préalables aux zones de trafic, à la page 747
- Lignes directrices relatives aux zones de trafic, à la page 749
- Configurer une zone de trafic, à la page 750
- Supervision des zones de trafic, à la page 751
- Exemple de zones de trafic, à la page 753
- Historique des zones de trafic, à la page 756

À propos des zones de trafic

Cette section décrit comment vous devez utiliser les zones de trafic dans votre réseau.

Comportement non zoné

L'algorithme de sécurité adaptatif prend en compte l'état d'un paquet lorsqu'il décide d'autoriser ou de refuser le trafic. L'un des paramètres appliqués pour le flux est que le trafic entre et sort de la même interface. Tout trafic pour un flux existant qui entre dans une interface différente est abandonné par l'ASA.

Les zones de trafic vous permettent de regrouper plusieurs interfaces afin que le trafic entrant ou sortant de *n'importe* quelle interface de la zone soit soumis aux contrôles de sécurité de l'algorithme de sécurité adaptatif.

Sujets connexes

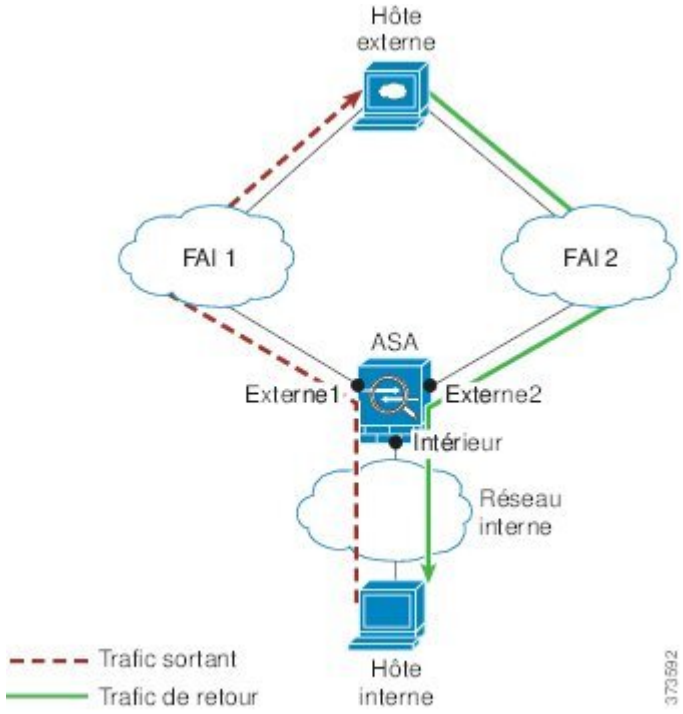
Présentation de l'inspection dynamique, à la page 13

Pourquoi utiliser des zones?

Vous pouvez utiliser des zones pour vous servir de plusieurs scénarios de routage.

Routage asymétrique

Dans le scénario suivant, une connexion a été établie entre un hôte interne et un hôte externe par le biais du FAI 1 sur l'interface Externe1. En raison d'un routage asymétrique sur le réseau de destination, le trafic de retour est arrivé du FAI 2 sur l'interface Externe2.

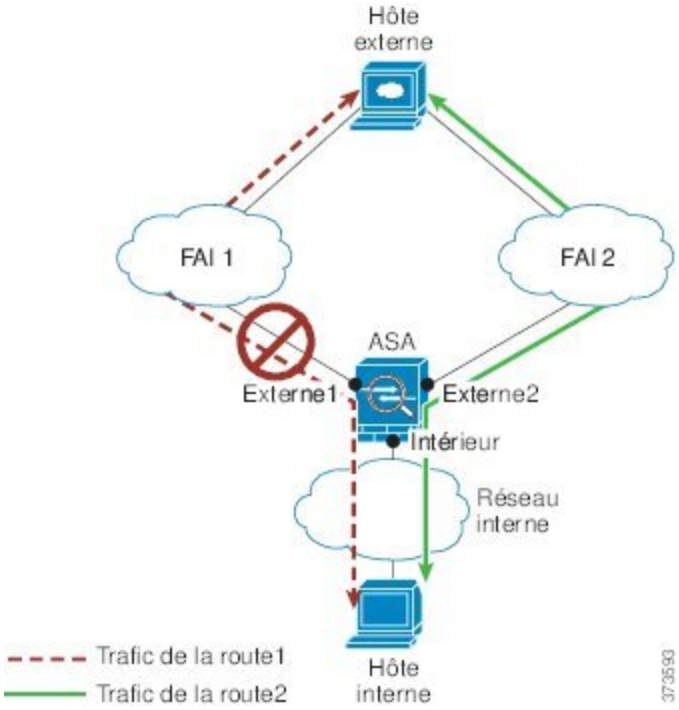


Problème non zoné : l'ASA gère les tables de connexion par interface. Lorsque le trafic de retour arrivera à Externe2, il ne correspondra pas à la table de connexion et sera abandonné. Pour une grappe ASA, le routage asymétrique lorsque la grappe a plusieurs contiguïtés avec le même routeur peut entraîner une perte de trafic inacceptable.

Solution zonée : l'ASA gère les tables de connexion par zone. Si vous regroupez Externe1 et Externe2 dans une zone, lorsque le trafic de retour arrivera à Externe2, il correspondra à la table de connexion par zone et la connexion sera autorisée.

Route perdue

Dans le scénario suivant, une connexion a été établie entre un hôte interne et un hôte externe par le biais du FAI 1 sur l'interface Externe1. En raison d'une route perdue ou déplacée entre Externe1 et le FAI 1, le trafic doit emprunter une route différente par le FAI 2.

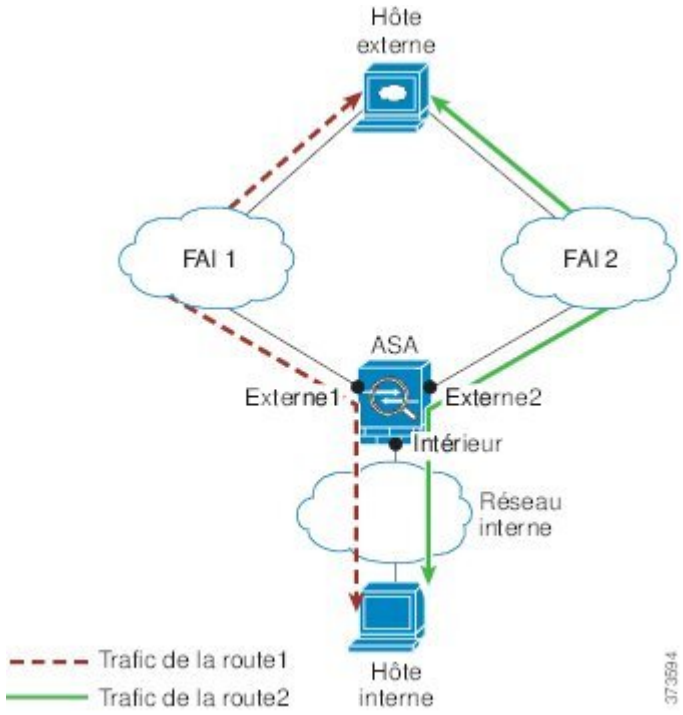


Problème non zoné : la connexion entre les hôtes interne et externe sera supprimée; une nouvelle connexion doit être établie à l'aide d'une nouvelle route optimale. Pour UDP, la nouvelle route sera utilisée après un seul abandon de paquet, mais pour TCP, une nouvelle connexion doit être rétablie.

Solution zonée : l'ASA détecte la route perdue et commute le flux dans le nouveau chemin par le biais du FAI 2. Le trafic sera transféré de manière transparente sans aucun abandon de paquets.

Équilibrage de la charge

Dans le scénario suivant, une connexion a été établie entre un hôte interne et un hôte externe par le biais du FAI 1 sur l'interface Externe1. Une deuxième connexion a été établie par le biais d'une route à coût égal par le biais du FAI 2 sur l'interface Externe2.



Problème non zoné : l'équilibrage de charges sur les interfaces n'est pas possible; vous ne pouvez équilibrer la charge qu'avec des routes à coût égal sur une interface.

Solution zonée : l'ASA équilibre les connexions sur un maximum de huit routes à coût égal sur toutes les interfaces de la zone.

Tables de connexion et de routage par zone

L'ASA gère une table de connexion par zone afin que le trafic puisse arriver sur n'importe quelle interface de zone. L'ASA gère également une table de routage par zone pour la prise en charge ECMP.

Routage ECMP

L'ASA prend en charge le routage à chemins multiples à coûts égaux (ECMP).

Prise en charge ECMP non zonée

Sans zones, vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal par interface. Par exemple, vous pouvez configurer trois routes par défaut sur l'interface externe qui spécifient différentes passerelles :

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

Dans ce cas, le trafic est équilibré en charge sur l'interface externe entre 10.1.1.2, 10.1.1.3 et 10.1.1.4. Le trafic est réparti entre les passerelles précisées selon un algorithme qui procède au hachage des adresses IP source et de destination, de l'interface entrante, du protocole et des ports source et destination.

Le protocole ECMP n'est pas pris en charge sur plusieurs interfaces; vous ne pouvez donc pas définir de route vers la même destination sur une interface différente. La route suivante n'est pas autorisée lorsqu'elle est configurée avec l'une des routes ci-dessus :

```
route outside2 0 0 10.2.1.1
```

Prise en charge ECMP zonée

Avec les zones, vous pouvez avoir jusqu'à 8 voies de routage statiques ou dynamiques de coût égal sur 8 interfaces au maximum dans une zone.

Lorsque ECMP détermine la répartition du trafic, il voit chaque interface d'accès virtuelle comme un seul participant ou option de chemin, même si cette interface d'accès virtuelle est associée à une interface qui a plusieurs adresses IPv6.

Par exemple, vous pouvez configurer trois routes par défaut sur trois interfaces dans la zone :

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

De même, votre protocole de routage dynamique peut configurer automatiquement des routes à coût égal. L'ASA équilibre la charge du trafic entre les interfaces grâce à un mécanisme d'équilibrage de la charge plus robuste.

Lorsqu'un routage est perdu, l'ASA déplace le flux de manière transparente vers une autre route.

Équilibrage de charges des connexions

L'ASA équilibre la charge des connexions sur des routes à coût égal à l'aide d'un hachage effectué à partir du paquet à six tuples (adresses IP source et de destination, port de destination, protocole et interface d'entrée). À moins que la route ne soit perdue, une connexion restera sur l'interface choisie pendant sa durée.

Les paquets d'une connexion ne sont pas équilibrés en charge sur toutes les routes; une connexion utilise une seule route, sauf si cette route est perdue.

L'ASA ne prend pas en compte la bande passante de l'interface ni d'autres paramètres lors de l'équilibrage de charges. Vous devez vous assurer que toutes les interfaces de la même zone ont les mêmes caractéristiques telles que la MTU, la bande passante, etc.

L'algorithme d'équilibrage de charges n'est pas configurable par l'utilisateur.

Basculement vers une route dans une autre zone

Lorsqu'une route est perdue sur une interface, s'il n'y a aucune autre route disponible dans la zone, l'ASA utilisera une route d'une interface ou d'une zone différente. Si cette route de secours est utilisée, vous pouvez rencontrer des abandons de paquet comme avec la prise en charge du routage non zoné.

Politique de sécurité basée sur l'interface

Les zones permettent le trafic vers et en provenance de n'importe quelle interface de la zone, mais la politique de sécurité elle-même (critères d'accès, NAT, etc.) est toujours appliquée par interface et non par zone. Si vous configurez la même politique de sécurité pour toutes les interfaces de la zone, vous pouvez alors mettre

en œuvre avec succès l'ECMP et l'équilibrage de charges pour ce trafic. Pour en savoir plus sur la configuration d'interface parallèle requise, consultez Conditions préalables aux zones de trafic, à la page 747.

Services pris en charge pour les zones de trafic

Les services suivants sont pris en charge avec les zones :

- Règles d'accès
- NAT
- Règles de service, à l'exception du contrôle de trafic QoS.
- Routage

Vous pouvez également configurer les services vers et à partir de la boîte répertoriés dans Trafic entrant et sortant, à la page 747, bien que la prise en charge complète des zones ne soit pas disponible.

Ne configurez pas d'autres services (comme le VPN ou le filtre de trafic de réseau de zombies) pour les interfaces dans une zone de trafic; elles peuvent ne pas fonctionner ou évoluer comme prévu.



Remarque Pour obtenir des renseignements détaillés sur la configuration de la politique de sécurité, consultez Conditions préalables aux zones de trafic, à la page 747.

Niveaux de sécurité

La première interface que vous ajoutez à une zone détermine le niveau de sécurité de la zone. Toutes les interfaces supplémentaires doivent avoir le même niveau de sécurité. Pour modifier le niveau de sécurité des interfaces d'une zone, vous devez supprimer toutes les interfaces sauf une, puis modifier les niveaux de sécurité et rajouter les interfaces.

Interface principale et actuelle pour le flux

Chaque flux de connexion est créé en fonction des interfaces d'entrée et de sortie initiales. Ces interfaces sont les interfaces *principales*.

Si une nouvelle interface de sortie est utilisée en raison de modifications de routes ou d'un routage asymétrique, les nouvelles interfaces sont les interfaces *actuelles*.

Rejoindre ou quitter une zone

Lorsque vous affectez une interface à une zone, toutes les connexions sur cette interface sont supprimées. Les connexions doivent être rétablies.

Si vous supprimez une interface d'une zone, toutes les connexions qui ont l'interface comme interface principale sont supprimées. Les connexions doivent être rétablies. Si l'interface est l'interface actuelle, l'ASA ramène les connexions à l'interface principale. La table de routage de zone est également actualisée.

Trafic intra-zone

Pour permettre au trafic d'*entrer* dans une interface et d'en *sortir*par une autre dans la même zone, activez **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Enable traffic between two or more hosts connected to the same interface (Activer le trafic entre deux hôtes ou plus connectés à la même interface)**, qui permet au trafic d'entrer et de sortir de la même interface, ainsi que **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Enable traffic between two or more interfaces which are configured with same security level (Activer le trafic entre deux interfaces ou plus qui sont configurées avec le même niveau de sécurité)**, qui autorise le trafic entre les interfaces de même sécurité. Sinon, un flux ne peut pas être acheminé entre deux interfaces dans la même zone.

Trafic entrant et sortant

- Vous ne pouvez pas ajouter des interfaces de gestion uniquement ou d'accès de gestion à une zone.
- Pour le trafic de gestion sur les interfaces régulières d'une zone, seul le routage asymétrique sur les flux existants est pris en charge; il n'y a pas de prise en charge ECMP.
- Vous ne pouvez configurer un service de gestion que sur une seule interface de zone, mais pour profiter de la prise en charge du routage asymétrique, vous devez le configurer sur toutes les interfaces. Même lorsque les configurations sont parallèles sur toutes les interfaces, ECMP n'est pas pris en charge.
- L'ASA prend en charge les services entrant et sortant suivants dans une zone :
  - Telnet
  - SSH
  - HTTPS
  - SNMP
  - Journal système

Chevauchement d'adresses IP dans une zone

Pour les interfaces non zonées, l'ASA prend en charge les réseaux d'adresses IP qui se chevauchent sur les interfaces tant que vous configurez la NAT correctement. Cependant, les réseaux qui se chevauchent ne sont pas pris en charge sur les interfaces de la même zone.

Conditions préalables aux zones de trafic

- Configurez tous les paramètres d'interface, y compris le nom, l'adresse IP et le niveau de sécurité. Notez que le niveau de sécurité doit correspondre pour toutes les interfaces de la zone. Il est conseillé de regrouper les interfaces similaires en termes de bande passante et d'autres propriétés de couche 2.
- Configurez les services suivants pour qu'ils correspondent sur toutes les interfaces de zone :
  - Critères d'accès : appliquez le même critère d'accès à toutes les interfaces membres de la zone ou utilisez un critère d'accès global.

Par exemple :

```
access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
access-group ZONE1 in interface outside1
access-group ZONE1 in interface outside2
access-group ZONE1 in interface outside3
```

- NAT : configurez la même politique NAT sur toutes les interfaces membres de la zone ou utilisez une règle NAT globale (en d'autres termes, utilisez « any » pour représenter les interfaces dans la règle NAT).

  L'interface PAT n'est pas prise en charge.

  Par exemple :

```
object network WEBSERVER1
  host 10.9.9.9 255.255.255.255
  nat (inside,any) static 209.165.201.9
```

Remarque Lorsque vous utilisez des ensembles NAT et PAT spécifiques à l'interface, l'ASA ne peut pas commuter les connexions en cas de défaillance de l'interface d'origine.

Si vous utilisez des ensembles PAT spécifiques à l'interface, plusieurs connexions du même hôte peuvent équilibrer la charge vers différentes interfaces et utiliser différentes adresses IP mappées. Les services Internet qui utilisent plusieurs connexions simultanées peuvent ne pas fonctionner correctement dans ce cas.

- Règles de service : utilisez la politique de service globale ou attribuez la même politique à chaque interface d'une zone.

  Le contrôle de trafic QoS n'est pas pris en charge.

  Par exemple :

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```

Remarque Pour les inspections VoIP, l'équilibrage de charges de la zone peut entraîner une augmentation des paquets désordonnés. Cette situation peut se produire, car les paquets ultérieurs peuvent atteindre l'ASA avant les paquets antérieurs qui empruntent un chemin différent. Les symptômes des paquets désordonnés sont les suivants :

- Utilisez la mémoire plus élevée aux nœuds intermédiaires (pare-feu et IDS) et aux nœuds de réception de la file d'attente si la mise en file d'attente est utilisée.
- Mauvaise qualité vidéo ou vocale.

Pour maîtriser ces effets, nous vous conseillons d'utiliser les adresses IP uniquement pour la répartition de la charge pour le trafic VoIP.

- Configurez le routage en tenant compte des capacités de la zone ECMP.

Lignes directrices relatives aux zones de trafic

Mode pare-feu

Pris en charge uniquement en mode de pare-feu routé. Ne prend pas en charge le mode de pare-feu transparent ni les interfaces de groupe de ponts en mode routé.

Basculement

- Vous ne pouvez pas ajouter la liaison de basculement ou d'état à une zone.
- En mode de basculement actif/actif, vous pouvez attribuer une interface dans chaque contexte à un groupe de routage asymétrique (ASR). Ce service permet de restaurer le trafic renvoyé sur une interface similaire de l'unité homologue vers l'unité d'origine. Vous ne pouvez pas configurer à la fois des groupes ASR et des zones de trafic dans un contexte. Si vous configurez une zone dans un contexte, aucune des interfaces de contexte ne peut faire partie d'un groupe ASR. Consultez Configurer la prise en charge des paquets routés asymétriques (mode actif/actif), à la page 331 pour de plus amples renseignements sur les groupes ASR.
- Seules les interfaces principales de chaque connexion sont répliquées sur l'unité en veille; les interfaces actuelles ne sont pas répliquées. Si l'unité en veille devient active, elle attribuera une nouvelle interface actuelle, au besoin.

Mise en grappe

- Vous ne pouvez pas ajouter la liaison de commande de grappe à une zone.

Directives sur les modèles

Vous ne pouvez pas ajouter les ports de commutation ni les interfaces VLAN de Firepower 1010 à une zone.

Directives supplémentaires

- Vous pouvez créer un maximum de 256 zones.
- Vous pouvez ajouter les types d'interfaces suivants à une zone :
  - Physique
  - VLAN
  - EtherChannel
- Vous ne pouvez pas ajouter les types d'interfaces suivants :
  - Gestion uniquement
  - Accès de gestion
  - Liaison de basculement ou d'état
  - Liaison de commande de la grappe
  - Interfaces membres dans un EtherChannel
  - VNI; de plus, si une interface de données standard est marquée comme nve-only, elle ne peut pas être membre d'une zone.
  - BVI ou interfaces membres d'un groupe de ponts.
- Une interface ne peut être membre que d'une seule zone.
- Vous pouvez inclure jusqu'à 8 interfaces par zone.
- Pour ECMP, vous pouvez ajouter jusqu'à 8 routes à coût égal par zone, sur toutes les interfaces de zone. Vous pouvez également configurer plusieurs routes sur une seule interface dans le cadre de la limite de 8 routes.
- Lorsque vous ajoutez une interface à une zone, toutes les routes statiques de ces interfaces sont supprimées.
- Vous ne pouvez pas activer le relais DHCP sur une interface dans une zone de trafic.
- L'ASA ne prend pas en charge le réassemblage des paquets fragmentés pour les fragments dont la charge est équilibrée sur des interfaces distinctes; ces fragments seront abandonnés.
- Le routage de multidiffusion PIM/IGMP n'est pas pris en charge sur les interfaces dans une zone.

Configurer une zone de trafic

Configurez une zone nommée et affectez des interfaces à la zone.

Procédure

Étape 1 Choisissez**Configuration** > **Configuration du périphérique** > **Paramètres de l'interface** > **Zones**, et cliquez sur **Ajouter**.

Vous pouvez choisir d'affecter une interface à une zone à partir de la boîte de dialogue **Configuration > Configuration du périphérique > Paramètres d'interface > Interfaces > Ajouter une interface**.

Étape 2 Le nom de la zone peut comporter jusqu'à 48 caractères.

Étape 3 Ajouter une ou plusieurs interfaces à l'espace **membre**. Assurez-vous que toutes les interfaces ont le même niveau de sécurité.

Étape 4 Cliquez sur **Apply** (Appliquer).

Supervision des zones de trafic

Cette section décrit comment superviser les zones de trafic.

Renseignements sur la zone

- **show zone** [*name*]

  Affiche l'ID de zone, le contexte, le niveau de sécurité et les membres.

  Consultez la sortie suivante pour la commande **show zone** :

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

- **show nameif zone**

  Affiche les noms d'interface et les noms de zone.

  Consultez la sortie suivante pour la commande **show nameif zone** :

```
ciscoasa# show nameif zone
Interface               Name                  zone-name      Security
GigabitEthernet0/0      inside-1              inside-zone     100
GigabitEthernet0/1.21   inside                inside-zone     100
GigabitEthernet0/1.31   4                                       0
GigabitEthernet0/2      outside               outside-zone   0
Management0/0           lan                                     0
```

Connexions de zone

- **show conn** [**long** | **detail**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

  La commande **show conn zone** affiche les connexions pour une zone. Les mots clés **long** et **detail** affichent l'interface principale sur laquelle la connexion a été établie, et celle entre parenthèses est l'interface actuellement utilisée pour transférer le trafic ou l'interface d'où provient le dernier paquet.

Ainsi, l'interface actuelle, dans le cas d'une connexion provenant de plusieurs interfaces, peut afficher différentes interfaces à différents moments selon le moment où la commande show conn a été émise.

Consultez la sortie suivante pour la commande **show conn long zone** :

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

  Affiche les tableaux de chemin de sécurité accélérés à des fins de débogage.

- **show local-host** [**zone** *zone_name* [**zone** *zone_name*] [...]]

  Affiche les états du réseau des hôtes locaux dans une zone.

  Consultez la sortie suivante pour la commande **show local-host zone**. L'interface principale est répertoriée en premier et l'interface actuelle est entre parenthèses.

```
ciscoasa# show local-host zone outside-zone

Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
 TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

Routage de zone

- **show route zone**

  Affiche les routes pour les interfaces de zone.

  Consultez la sortie suivante pour la commande **show route zone** :

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
```

```
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

- **show asp table routing**

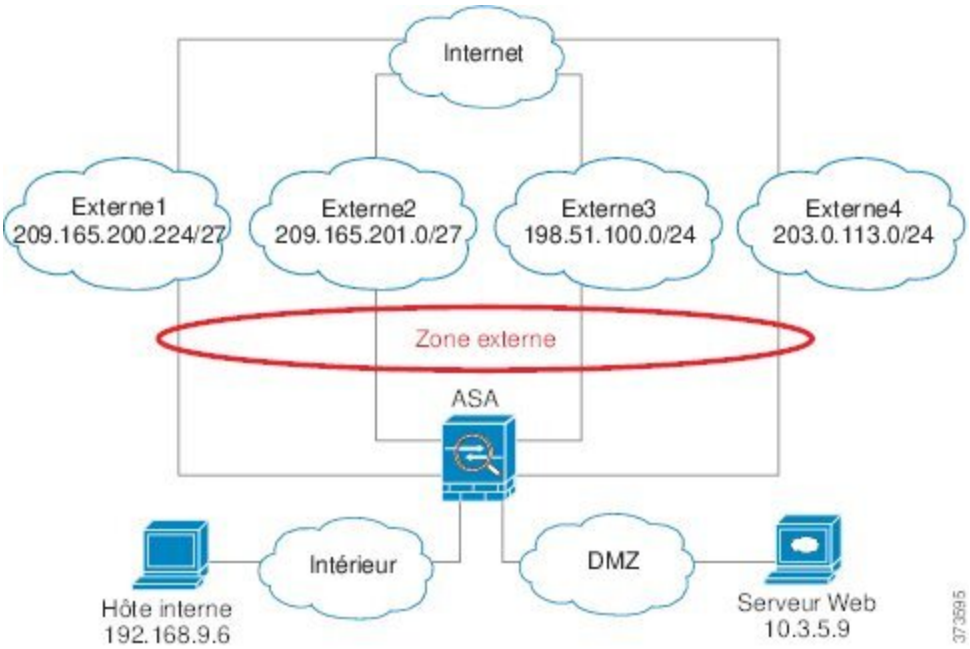
  Affiche les tableaux de chemins de sécurité accélérés à des fins de débogage et affiche la zone associée à chaque route.

  Consultez la sortie suivante pour la commande **show asp table routing** :

```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1       255.255.255.255 identity
in   10.2.0.1       255.255.255.255 identity
in   10.6.6.4         255.255.255.255 identity
in   10.4.4.4         255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in   172.0.0.67       255.255.255.255 identity
in   172.0.0.0       255.255.255.0   wan-zone:outside2
in   10.85.43.0      255.255.255.0   via 10.4.0.3 (unresolved, timestamp: 50)
in   10.85.45.0      255.255.255.0   via 10.4.0.20 (unresolved, timestamp: 51)
in   192.168.0.0        255.255.255.0   mgmt
in   192.168.1.0       255.255.0.0     lan-zone:inside
out  255.255.255.255 255.255.255.255 mgmt
out  172.0.0.67       255.255.255.255 mgmt
out  172.0.0.0        255.255.255.0   mgmt
out  10.4.0.0       240.0.0.0       mgmt
out  255.255.255.255 255.255.255.255 lan-zone:inside
out  10.1.0.1       255.255.255.255 lan-zone:inside
out  10.2.0.0       255.255.0.0     lan-zone:inside
out  10.4.0.0       240.0.0.0       lan-zone:inside
```

Exemple de zones de trafic

L’exemple suivant affecte 4 interfaces VLAN à la zone externe et configure 4 routes par défaut à coût égal. La PAT est configurée pour l’interface interne, et un serveur Web est disponible sur une interface DMZ à l’aide de la NAT statique.




```
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch

zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown
```

```
interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99

# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
```

```
    inspect rtsp
    inspect skinny
    inspect esmtp _default_esmtp_map
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
service-policy global_policy global
```

Historique des zones de trafic

Nom de la caractéristique	Versions de plateforme	Description
Zones de circulation	9.3(2)	Vous pouvez regrouper les interfaces dans une zone de trafic pour réaliser l'équilibrage de la charge de trafic (à l'aide du routage ECMP (chemins multiples à coût égal)), la redondance de routes et le routage asymétrique sur plusieurs interfaces. **Remarque** Vous ne pouvez pas appliquer de politique de sécurité à une zone nommée; la politique de sécurité est basée sur l'interface. Lorsque les interfaces d'une zone sont configurées avec un critère d'accès, une NAT et une politique de service identiques, l'équilibrage de charges et le routage asymétrique fonctionnent correctement. Nous avons introduit ou modifié les écrans suivants : **Configuration > Device Setup (Configuration de l'appareil) > Interface Parameters (Paramètres d'interface) > Zones** **Configuration > Device Setup (Configuration de l'appareil) > Interface Parameters (Paramètres d'interface) > Interfaces**.
commande **clear local-host**	9.14(1)	La commande **clear local-host** et tous ses attributs et ses mots clés étaient obsolètes. Ils seront supprimés dans une version ultérieure.



PARTIE IV

Paramètres de base

- Paramètres de base, à la page 759
- Services DHCP et DDNS, à la page 781
- Certificats numériques, à la page 803
- Inspection ARP et table des adresses MAC, à la page 835



CHAPITRE 24

Paramètres de base

Ce chapitre décrit comment configurer les paramètres de base sur l'ASA qui sont généralement requis pour une configuration fonctionnelle.

- Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet, à la page 759
- Régler la date et l'heure, à la page 761
- Configurer la phrase secrète principale, à la page 765
- Configurer des serveurs DNS, à la page 768
- Configurer le contournement matériel et l'alimentation double (Cisco ISA 3000), à la page 771
- Modifier les performances et le comportement ASP (Accelerated Security Path), à la page 773
- Supervision du cache DNS, à la page 775
- Historique des paramètres de base, à la page 776

Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet

Pour définir le nom d'hôte, le nom de domaine et les mots de passe d'activation et pour Telnet, procédez comme suit.

Avant de commencer

Avant de définir le nom d'hôte, le nom de domaine et les mots de passe d'activation et pour Telnet, assurez-vous les conditions préalables suivantes sont réunies :

- En mode contexte multiple, vous pouvez configurer le nom d'hôte et le nom de domaine dans les espaces d'exécution du système et du contexte.
- Les mots de passe d'activation et pour Telnet doivent être définis dans chaque contexte. Ils ne sont pas disponibles dans le système.
- Pour passer du système à une configuration de contexte, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Device Name/Password**.

Étape 2 Entrez le nom d'hôte. Le nom d'hôte par défaut est « ciscoasa ».

Le nom d'hôte apparaît dans l'invite de ligne de commande, et si vous établissez des sessions avec plusieurs appareils, celui-ci facilite le suivi de l'emplacement où vous entrez des commandes. Le nom d'hôte est également utilisé dans les messages syslog.

En mode contexte multiple, le nom d'hôte que vous avez défini dans l'espace d'exécution du système apparaît dans l'invite de ligne de commande de tous les contextes. Le nom d'hôte que vous définissez dans un contexte n'apparaît pas sur la ligne de commande. Il peut être utilisé pour une bannière.

Étape 3 Entrez le nom de domaine. Le nom de domaine par défaut est default.domain.invalid.

L'ASA ajoute le nom de domaine sous forme de suffixe aux noms non qualifiés. Par exemple, si vous définissez le nom de domaine « example.com » et indiquez un serveur syslog sous le nom non qualifié de « jupiter », l'ASA remplace ce nom par « jupiter.example.com ».

Étape 4 Changez le mot de passe (d'activation) du mode privilégié. Par défaut, le mot de passe d'activation est une valeur vide, mais vous êtes invité à la modifier la première fois que vous entrez la commande **enable** dans l'interface de ligne de commande.

Le mot de passe d'activation vous permet de passer en mode d'exécution privilégié si vous ne configurez pas l'authentification d'activation. Le mot de passe d'activation vous permet également de vous connecter à ASDM avec un nom d'utilisateur vide si vous ne configurez pas l'authentification HTTP. Contrairement à l'accès par l'interface de ligne de commande, ASDM n'oblige pas à modifier le mot de passe d'activation.

a) Cochez la case **Change the private mode password** pour modifier le mot de passe du mode privilégié.
b) Entrez puis entrez le nouveau mot de passe et confirmez-le. Définissez un mot de passe sensible à la casse de 8 à 127 caractères. Il peut s'agir de n'importe quelle combinaison de caractères imprimables ASCII (codes 32 à 126), avec les exceptions suivantes :

- Aucun espace
- Aucun point d'interrogation
- Il est interdit d'utiliser trois caractères ASCII (ou plus) qui se suivent ou qui se répètent. Par exemple, les mots de passe suivants seront refusés :
  - **abc**utilisateur1
  - utilisateur**543**
  - utilisateur**aaaa**
  - utilisateur2**666**

Vous ne pouvez pas réinitialiser le mot de passe à une valeur vide.

Étape 5 Définissez le mot de passe de connexion pour l'accès Telnet. Il n'y a pas de mot de passe par défaut.

Le mot de passe de connexion est utilisé pour l'accès Telnet si vous ne configurez pas l'authentification Telnet.

a) Cochez la case **Change the password to access the console of the security appliance** pour changer le mot de passe pour accéder à la console de l'appareil de sécurité.
b) Entrez l'ancien mot de passe (pour un nouvel ASA, laissez ce champ vide), puis entrez le nouveau mot de passe et confirmez-le. Le mot de passe peut comporter jusqu'à 16 caractères. Il peut s'agir de n'importe quelle combinaison de caractères imprimables ASCII (codes 32 à 126), à l'exception des espaces et du point d'interrogation.

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Régler la date et l'heure



Remarque Ne définissez pas la date et l'heure de de Firepower 2100 en mode plateforme, 4100/9300; l'ASA reçoit ces paramètres du châssis.

Définir la date et l'heure à l'aide du serveur NTP

Le protocole NTP est utilisé pour mettre en œuvre un système hiérarchique de serveurs qui fournissent une heure synchronisée avec précision entre les systèmes du réseau. Ce type de précision est requis pour les opérations urgentes, telles que la validation de listes de révocation de certificats, qui comprennent un horodatage précis. Vous pouvez configurer plusieurs serveurs NTP. L'ASA choisit le serveur avec la strate la plus basse, qui est une mesure de la fiabilité des données.

L'heure dérivée d'un serveur NTP remplace toute heure définie manuellement.

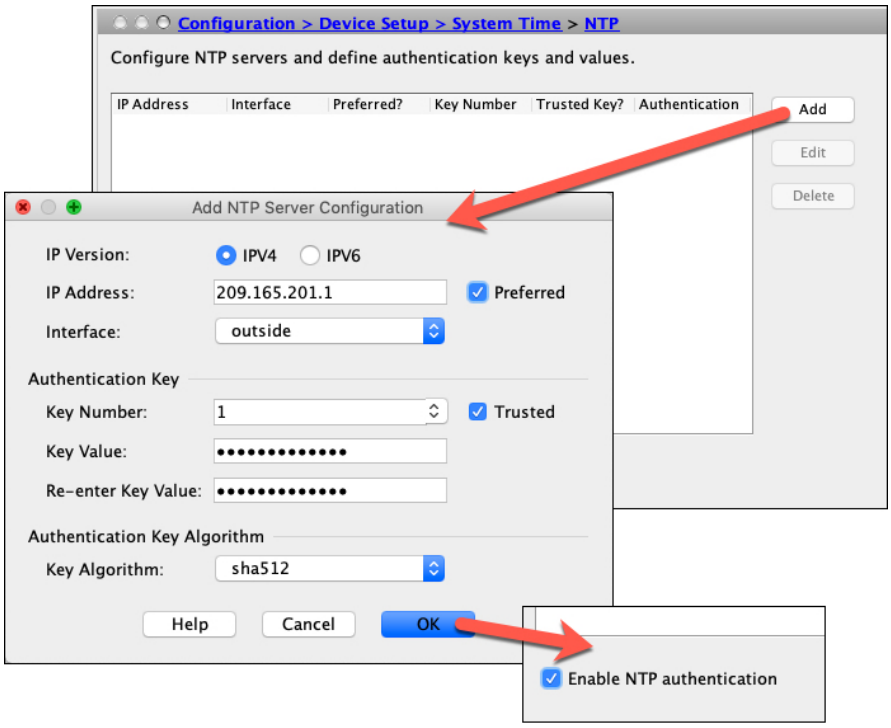
L'ASA prend en charge NTPv4.

Avant de commencer

En mode de contexte multiple, vous pouvez définir l'heure dans la configuration système uniquement.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **System Time (Heure du système)** > **NTP**.



Étape 2 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add NTP Server Configuration** (Ajouter une configuration de serveur NTP).

Étape 3 Saisissez l'**IPv4** ou **IPv6 IP Address** (Adresse IP IPv4 ou IPv6) du serveur NTP.

Vous ne pouvez pas saisir de nom d'hôte pour le serveur; l'ASA ne prend pas en charge la recherche DNS pour le serveur NTP.

Étape 4 (Facultatif) Cochez la case **Preferred** (Préféré) pour définir ce serveur comme serveur préféré.

Le NTP utilise un algorithme pour déterminer quel serveur est le plus précis et se synchronise avec lui. Si les serveurs ont la même précision, le serveur préféré est utilisé. Cependant, si un serveur est nettement plus précis que le serveur préféré, l'ASA utilise le plus précis.

Étape 5 (Facultatif) Choisissez **l'interface** dans la liste déroulante.

Ce paramètre spécifie l'interface sortante pour les paquets NTP. Si l'interface est vide, l'ASA utilise l'interface de contexte d'administration par défaut conformément à la table de routage de gestion.

Étape 6 (Facultatif) Configurez l'authentification NTP

a) Saisissez un **Key Number** (Numéro de clé) compris entre 1 et 4294967295, ou choisissez un numéro de clé existant dans la liste déroulante si vous avez précédemment créé une clé pour un autre serveur NTP que vous souhaitez réutiliser.

Ce paramètre spécifie l'ID de clé pour cette clé d'authentification, qui vous permet d'utiliser l'authentification pour communiquer avec le serveur NTP. Les paquets du serveur NTP doivent également utiliser cet ID de clé.

b) Cochez la case **Trusted** (Approuvé).

c) Saisissez la **Key Value** (Valeur de clé), qui est une chaîne de 32 caractères maximum, puis saisissez à nouveau la valeur de clé.

d) Sélectionnez un **Key Algorithm** (Algorithme de clé) dans la liste déroulante.
e) Cliquez sur **OK**.

Étape 7 Cochez la case **Enable NTP authentication** (Activer l'authentification NTP) pour activer l'authentification NTP.

Étape 8 Cliquez sur **Apply** pour enregistrer vos modifications.

Régler la date et l'heure manuellement

Pour définir la date et l'heure manuellement, procédez comme suit :

Avant de commencer

En mode de contexte multiple, vous pouvez définir l'heure dans la configuration système uniquement.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **System Time (Heure du système)** > **Clock (Horloge)**.

Étape 2 Choisissez le fuseau horaire dans la liste déroulante. Ce paramètre spécifie le fuseau horaire comme GMT plus ou moins le nombre d'heures approprié. Si vous sélectionnez le fuseau horaire de l'Est, de l'Heure Centrale, de l'Heure de montage ou de l'Heure du Pacifique, l'heure s'ajuste automatiquement pour l'heure avancée, de 2 h le deuxième dimanche de mars à 2 h le premier dimanche de novembre.

Remarque La modification du fuseau horaire de l'ASA peut interrompre la connexion aux SSM intelligents.

Étape 3 Cliquez sur la liste déroulante **Date** pour afficher un calendrier. Trouvez ensuite la bonne date en utilisant les méthodes suivantes :

- Cliquez sur le nom du mois pour afficher une liste des mois, puis cliquez sur le mois souhaité. Le calendrier se met à jour pour ce mois.
- Cliquez sur l'année pour changer d'année. Utilisez les flèches vers le haut et le bas pour faire défiler les années ou saisissez une année dans le champ de saisie.
- Cliquez sur les flèches vers la droite et la gauche du mois et de l'année pour faire défiler le calendrier vers l'avant et l'arrière d'un mois à la fois.
- Cliquez sur un jour du calendrier pour définir la date.

Étape 4 Saisissez la durée manuellement en heures, en minutes et en secondes.

Étape 5 Cliquez sur **Update Display Time** (Mettre à jour l'heure d'affichage) pour mettre à jour l'heure affichée dans le coin inférieur droit du volet ASDM. L'heure actuelle est mise à jour automatiquement toutes les dix secondes.

Configurer le protocole PTP (Precision Time Protocol) (ISA 3000)

Le protocole PTP (Precision Time Protocol) est un protocole de synchronisation horaire développé pour synchroniser les horloges de divers périphériques au sein d'un réseau par paquets. Ces horloges sont généralement de précision et de stabilité variables. Le protocole est spécialement conçu pour les systèmes de mesure et de contrôle industriels en réseau. Il est idéal pour une utilisation dans les systèmes distribués, car il nécessite une bande passante et un surdébit de traitement minimaux.

Un système PTP est un système en réseau distribué, composé d'une combinaison de périphériques PTP et non-PTP. Les périphériques PTP comprennent les horloges normales, les horloges périphériques et les horloges transparentes. Les périphériques non PTP comprennent les commutateurs réseau, les routeurs et les autres périphériques de l'infrastructure.

Vous pouvez configurer l'ASA pour qu'il soit une horloge transparente. L'ASA ne synchronise pas son horloge avec les horloges PTP. L'ASA utilisera le profil PTP par défaut, comme défini sur les horloges PTP.

Lorsque vous configurez les périphériques PTP, vous définissez un numéro de domaine pour les périphériques qui sont destinés à fonctionner ensemble. Ainsi, vous pouvez configurer plusieurs domaines PTP, puis configurer chaque périphérique non PTP pour qu'il utilise les horloges PTP d'un domaine spécifique.

Avant de commencer

- Cette fonctionnalité est uniquement disponible sur l'ISA 3000.
- L'utilisation du PTP n'est prise en charge qu'en mode de contexte unique.
- Cisco PTP prend uniquement en charge les messages PTP en multidiffusion.
- Le PTP est activé sur toutes les interfaces ISA 3000 en mode transparent par défaut. En mode routé, vous devez ajouter la configuration nécessaire pour vous assurer que les paquets PTP sont autorisés à transiter par le périphérique.
- Le PTP est disponible uniquement pour les réseaux IPv4, et non pour les réseaux IPv6.
- La configuration PTP est prise en charge sur les interfaces Ethernet physiques, qu'elles soient autonomes ou membres d'un groupe de ponts. Elle n'est pas prise en charge sur :
  - Interface de gestion.
  - Sous-interfaces, EtherChannels, BVI ou toute autre interface virtuelle.
- Les flux PTP sur les sous-interfaces VLAN sont pris en charge, en supposant que la configuration PTP appropriée est présente sur l'interface parente.
- Vous devez vous assurer que les paquets PTP sont autorisés à circuler dans le périphérique. En mode de pare-feu transparent, la configuration de la liste d'accès permettant le trafic PTP est configurée par défaut. Le trafic PTP est identifié par les ports UDP 319 et 320 et par l'adresse IP de destination 224.0.1.129. Ainsi, en mode de pare-feu routé, toute liste ACL autorisant ce trafic devrait être acceptable.
- En mode de pare-feu routé, vous devez également activer le routage de multidiffusion pour les groupes de multidiffusion PTP :
  - Entrez la commande du mode de configuration globale **multicast-routing**.
  - Et pour chaque interface qui n'est pas membre d'un groupe de ponts et sur laquelle le protocole PTP est activé, saisissez la commande de configuration d'interface **igmp join-group 224.0.1.129**

pour activer statiquement l'appartenance au groupe de multidiffusion PTP. Cette commande n'est pas prise en charge ni nécessaire pour les membres du groupe de ponts.

Procédure

Étape 1 Sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **PTP**.

Étape 2 Renseignez le champ **Domain value** (Valeur du domaine).

Il s'agit du numéro de domaine pour tous les ports du périphérique. Les paquets reçus dans un domaine différent sont traités comme des paquets de multidiffusion ordinaires et ne subissent aucun traitement PTP. Cette valeur peut aller de zéro à 255; la valeur par défaut est zéro. Saisissez le numéro de domaine configuré sur les périphériques PTP de votre réseau.

Étape 3 (Facultatif) Sélectionnez **Enable End-to-End Transparent Clock Mode** (Activer le mode d'horloge transparent de bout en bout) pour activer le mode transparent de bout en bout sur toutes les interfaces compatibles avec PTP.

Une horloge transparente est une horloge qui compense ses retards en mesurant les temps de résidence et en mettant à jour le champ `correctionField` dans le paquet PTP.

Étape 4 Activez PTP sur une ou plusieurs interfaces de périphérique en sélectionnant une interface et en cliquant sur **Enable** (Activer) ou **Disable** (Désactiver).

Activez PTP sur chaque interface par laquelle le système peut communiquer avec une horloge PTP dans le domaine configuré.

Étape 5 Cliquez sur **Apply** (Appliquer).

Prochaine étape

Vous pouvez sélectionner **Monitoring (Supervision)** > **Properties (Propriétés)** > **PTP** pour afficher les renseignements relatifs à l'horloge PTP et à l'interface/au port.

Configurer la phrase secrète principale

La phrase secrète principale vous permet de stocker en toute sécurité les mots de passe en texte brut dans un format chiffré et fournit une clé utilisée pour chiffrer ou masquer tous les mots de passe de manière universelle, sans modifier aucune fonctionnalité. Voici les fonctionnalités qui utilisent la phrase secrète principale :

- OSPF
- EIGRP
- Équilibrage de la charge VPN
- VPN (accès à distance et de site à site)
- Basculement
- Serveurs AAA

- Logging (journalisation)
- Licences partagées

Ajouter ou modifier la phrase secrète principale

Pour ajouter ou modifier la phrase secrète principale, procédez comme suit.

Avant de commencer

- Cette procédure ne sera acceptée que dans une session sécurisée, par exemple par la console, SSH ou ASDM via HTTPS.
- Si le basculement est activé, mais qu'aucune clé partagée de basculement n'est définie, un message d'erreur s'affiche si vous modifiez la phrase secrète principale, vous informant que vous devez saisir une clé partagée de basculement pour protéger les modifications de phrase secrète principale contre l'envoi en texte brut.

  Choisissez **Configuration > Device Management (Gestion des périphériques) > High Availability (Haute disponibilité) > Failover (Basculement)**, saisissez un caractère dans le champ **Shared Key** (Clé partagée) ou 32 chiffres hexadécimaux (0-9A-Fa-f) si une clé hexadécimale de basculement est sélectionnée, à l'exception de la touche retour arrière. Cliquez ensuite sur **Apply** (Appliquer).
- L'activation ou la modification du chiffrement par mot de passe dans le basculement actif/veille entraîne un **write standby**, qui réplique la configuration active sur l'unité de secours. Sans cette réplication, les mots de passe chiffrés sur l'unité de secours seront différents, même s'ils utilisent la même phrase secrète; la réplication de la configuration garantit que les configurations sont identiques. Pour le basculement actif/actif, vous devez saisir manuellement **write standby**. Un **write standby** peut entraîner une interruption du trafic en mode actif/actif, car la configuration est effacée sur l'unité secondaire avant que la nouvelle configuration ne soit synchronisée. Vous devez activer tous les contextes sur l'ASA principal à l'aide des commandes **failover active group 1** et **failover active group 2**, saisir **write standby**, puis restaurer les contextes du groupe 2 sur l'unité secondaire à l'aide de la commande **no failover active group 2**.

Procédure

Étape 1 Choisissez une des options suivantes :

- En mode de contexte unique, choisissez **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Master Passphrase (Phrase secrète principale)**.
- En mode de contexte multiple, choisissez **Configuration > Device Management (Gestion des périphériques) > Device Administration (Administration des périphériques) > Master Passphrase (Phrase secrète principale)**.

Étape 2 Cochez la case **Advanced Encryption Standard (AES) password encryption** (Chiffrement du mot de passe AES (norme de chiffrement avancé)).

Si aucune phrase secrète principale n'est en vigueur, un message d'avertissement s'affiche lorsque vous cliquez sur Apply (Appliquer). Vous pouvez cliquer sur OK ou Cancel (Annuler) pour continuer.

Si vous désactivez ultérieurement le chiffrement des mots de passe, tous les mots de passe chiffrés existants resteront inchangés et, tant que la phrase secrète principale existe, les mots de passe chiffrés seront déchiffrés, comme l'exige l'application.

Étape 3 Cochez la case **Change the encryption master passphrase** (Modifier la phrase secrète principale de chiffrement) pour pouvoir saisir et confirmer vos nouvelles phrases secrètes principales. Par défaut, elles sont désactivées.

Votre nouvelle phrase secrète principale doit comporter entre 8 et 128 caractères.

Si vous modifiez une phrase secrète existante, vous devez saisir l'ancienne phrase secrète avant de pouvoir en saisir une nouvelle.

Laissez les champs **New** (Nouveau) et **Confirm Master passphrase** (Confirmer la phrase secrète principale) vides pour supprimer la phrase secrète principale.

Étape 4 Cliquez sur **Apply** (Appliquer).

Désactiver la phrase secrète principale

La désactivation de la phrase secrète principale rétablit les mots de passe chiffrés en mots de passe en texte brut. Supprimer la phrase secrète peut être utile si vous rétrogradez à une version précédente du logiciel qui ne prend pas en charge les mots de passe chiffrés.

Avant de commencer

- Vous devez connaître la phrase secrète principale actuelle pour la désactiver.
- Cette procédure fonctionne uniquement dans une session sécurisée; c'est-à-dire par Telnet, SSH ou ASDM via HTTPS.

  Pour désactiver la phrase secrète principale, procédez comme suit :

Procédure

Étape 1 Choisissez une des options suivantes :

- En mode de contexte unique, choisissez **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Master Passphrase (Phrase secrète principale)**.
- En mode de contexte multiple, choisissez **Configuration > Device Management (Gestion des périphériques) > Device Administration (Administration des périphériques) > Master Passphrase (Phrase secrète principale)**.

Étape 2 Cochez la case **Advanced Encryption Standard (AES) password encryption** (Chiffrement du mot de passe AES (norme de chiffrement avancé)).

Si aucune phrase secrète principale n'est en vigueur, une instruction d'avertissement s'affiche lorsque vous cliquez sur Apply (Appliquer). Cliquez sur OK ou Cancel (Annuler) pour continuer.

Étape 3 Cochez la case Change the encryption master passphrase (Modifier la phrase secrète principale de chiffrement).

Étape 4 Saisissez l'ancienne phrase secrète principale dans le champ **Old master passphrase** (Ancienne phrase secrète principale). Vous devez fournir l'ancienne phrase secrète principale pour la désactiver.

Étape 5 Laissez les champs **New Master passphrase** (Nouvelle phrase secrète principale) et **Confirm Master passphrase** (Confirmer la phrase secrète principale) vides.

Étape 6 Cliquez sur **Apply** (Appliquer).

Configurer des serveurs DNS

Vous devez configurer un serveur DNS pour que l'ASA puisse résoudre les noms d'hôte en adresses IP. Vous devez également configurer un serveur DNS pour utiliser des objets réseau de noms de domaine complets (FQDN) dans les critères d'accès.

Certaines fonctionnalités de l'ASA nécessitent l'utilisation d'un serveur DNS pour accéder aux serveurs externes par nom de domaine. D'autres fonctionnalités, telles que la commande **ping** ou **traceroute**, vous permettent de saisir un nom que vous souhaitez envoyer par message Ping ou par route de trace. L'ASA peut résoudre le nom en communiquant avec un serveur DNS. De nombreuses commandes SSL VPN et de certificat prennent également en charge les noms.

Par défaut, il existe un groupe de serveurs DNS par défaut appelé DefaultDNS. Vous pouvez créer plusieurs groupes de serveurs DNS : un groupe est le groupe par défaut, tandis que les autres groupes peuvent être associés à des domaines spécifiques. Une requête DNS qui correspond à un domaine associé à un groupe de serveurs DNS utilisera ce groupe. Par exemple, si vous souhaitez que le trafic destiné aux serveurs internes eng.cisco.com utilise un serveur DNS interne, vous pouvez mapper eng.cisco.com à un groupe DNS interne. Toutes les requêtes DNS qui ne correspondent pas à un mappage de domaine utiliseront le groupe de serveurs DNS par défaut, qui n'a pas de domaine associé. Par exemple, le groupe DefaultDNS peut inclure un serveur DNS public disponible sur l'interface externe. D'autres groupes de serveurs DNS peuvent être configurés pour les groupes de tunnels VPN. Consultez la commande **tunnel-group** dans la référence de commande pour en savoir plus.

Remarque L'ASA a une prise en charge limitée pour l'utilisation du serveur DNS, en fonction de la fonctionnalité.

Avant de commencer

Assurez-vous de configurer les règles de routage et d'accès appropriées pour toute interface sur laquelle vous activez la recherche de domaine DNS afin de pouvoir atteindre le serveur DNS.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**.

Étape 2 Choisissez l'une des options suivantes dans la zone **DNS Setup** (Configuration DNS) :

- **Configure one DNS server group** (Configurer un groupe de serveurs DNS) : cette option définit les serveurs du groupe DefaultDNS.

- **Configure multiple DNS server groups** (Configurer plusieurs groupes de serveurs DNS) : avec cette option, vous pouvez configurer le groupe DefaultDNS ainsi que d'autres groupes que vous pouvez associer à des domaines spécifiques et des groupes à utiliser avec les stratégies de groupe SSL VPN d'accès à distance. Même si vous configurez uniquement le groupe DefaultDNS, vous devez sélectionner cette option si vous souhaitez modifier le délai d'expiration et d'autres caractéristiques utilisées avec le groupe.

Étape 3 Si vous sélectionnez **Configure one DNS server group** (Configurer un groupe de serveurs DNS), configurez les serveurs dans le groupe DefaultDNS.

a) Dans **Primary DNS Server** (Serveur DNS principal), saisissez l'adresse IP du serveur DNS qui doit être utilisé chaque fois qu'il est disponible. Pour ce serveur et chaque serveur secondaire, spécifiez éventuellement le *nom d'interface* par lequel l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage des données; s'il n'y a aucune correspondance, il vérifie la table de routage de gestion uniquement.

b) Cliquez sur **Add** (Ajouter) pour ajouter des serveurs DNS secondaires.

Vous pouvez ajouter jusqu'à six serveurs DNS. L'ASA essaie chaque serveur DNS dans l'ordre jusqu'à ce qu'il reçoive une réponse. Utilisez les boutons **Move Up** (Déplacer vers le haut)/**Move Down** (Déplacer vers le bas) pour classer les serveurs par ordre de priorité.

c) Saisissez un nom de domaine DNS ajouté au nom d'hôte s'il n'est pas entièrement qualifié.

Étape 4 Si vous sélectionnez **Configure multiple DNS server groups** (Configurer plusieurs groupes de serveurs DNS), définissez les propriétés du groupe de serveurs.

a) Cliquez sur **Add** (Ajouter) pour créer un nouveau groupe, ou sélectionnez un groupe et cliquez sur **Edit** (Modifier).

Le groupe DefaultDNS est toujours répertorié.

b) Configurez les propriétés du groupe.

- **Server IP Address to Add**, **Source Interface** (Adresse IP du serveur à ajouter, interface source) : saisissez l'adresse IP d'un serveur DNS et cliquez sur **Add>>** (Ajouter>>). Pour chaque serveur, spécifiez éventuellement le *nom d'interface* par lequel l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.

  Vous pouvez ajouter jusqu'à six serveurs DNS. L'ASA essaie chaque serveur DNS dans l'ordre jusqu'à ce qu'il reçoive une réponse. Utilisez les boutons **Move Up** (Déplacer vers le haut)/**Move Down** (Déplacer vers le bas) pour classer les serveurs par ordre de priorité.

- **Timeout** (Délai d'attente) : le nombre de secondes, de 1 à 30, à attendre avant d'essayer le serveur DNS suivant. La valeur par défaut est de 2 secondes. Chaque fois que l'ASA réessaie la liste des serveurs, ce délai est doublé.

- **Retries** (Nouvelles tentatives) : le nombre de tentatives, de 0 à 10, pour retenter d'accéder à la liste des serveurs DNS lorsque l'ASA ne reçoit pas de réponse.

- **Expire Entry Timer** (Délai d'expiration de l'entrée) (DefaultDNS ou groupe actif uniquement) : la TTL minimum pour l'entrée DNS, en minutes. Si le délai d'expiration est plus long que la durée de vie de l'entrée, cette dernière est augmentée jusqu'à la valeur du délai d'expiration de l'entrée. Si la durée de vie est plus longue que le délai d'expiration, la valeur du délai d'expiration est ignorée : dans ce cas, aucun délai supplémentaire n'est ajouté à la durée de vie. À l'expiration, l'entrée est supprimée de la table de consultation du DNS. La suppression d'une entrée nécessite la recompilation de la table, de sorte que des suppressions fréquentes peuvent augmenter la charge de traitement du

périphérique. Comme certaines entrées DNS peuvent avoir une durée de vie très courte (jusqu'à trois secondes), vous pouvez utiliser ce paramètre pour prolonger virtuellement cette dernière. La valeur par défaut est 1 minute (c'est-à-dire que la durée de vie minimale pour toutes les résolutions est de 1 minute). La plage est comprise entre 1 et 65535 minutes. Cette option est utilisée uniquement pour la résolution d'objets réseau FQDN.

- **Poll Timer** (Délai d'interrogation) (DefaultDNS ou groupe actif uniquement) : la durée, en minutes, du cycle d'interrogation utilisé pour résoudre les objets réseau/hôte FQDN en adresses IP. Les objets FQDN ne sont résolus que s'ils sont utilisés dans une politique de pare-feu. La minuterie détermine le temps maximum entre les résolutions; la valeur de durée de vie (TTL) de l'entrée DNS est également utilisée pour déterminer quand mettre à jour la résolution d'adresse IP, de sorte que les FQDN individuels puissent être résolus plus fréquemment que le cycle d'interrogation. La valeur par défaut est 240 (quatre heures). La plage est comprise entre 1 et 65535 minutes.
- **Domain Name** (Nom de domaine) (DefaultDNS ou groupe actif uniquement) : le nom de domaine ajouté au nom d'hôte s'il n'est pas entièrement qualifié.

c) Cliquez sur **OK**.

d) Si vous avez plusieurs groupes, vous pouvez modifier le groupe par défaut en le sélectionnant et en cliquant sur **Set Active** (Activer).

Vous ne pouvez utiliser un groupe comme valeur par défaut que s'il n'y a aucun domaine mappé à celui-ci (voir Étape 8, à la page 771).

Étape 5 Assurez-vous que la recherche DNS est activée sur au moins une interface. Dans la liste d'interfaces **DNS Lookup** (Recherche DNS), sous le tableau des groupes de serveurs DNS, cliquez dans la colonne **DNS Enabled** (DNS activé) et sélectionnez **True** (Vrai) pour activer la recherche sur l'interface.

Assurez-vous d'activer la recherche DNS sur toutes les interfaces qui seront utilisées pour accéder aux serveurs DNS.

Si vous n'activez pas la recherche DNS sur une interface, la **Source Interface** (Interface source) du serveur DNS ou l'interface trouvée à l'aide de la table de routage ne peut pas être utilisée.

Étape 6 (Facultatif) Sous **Trusted DNS Server** (Serveur DNS de confiance), configurez les options pour déterminer les serveurs de confiance lors de la résolution des noms de domaine dans les objets de service réseau.

a) (Facultatif) Ajoutez ou supprimez des serveurs DNS de confiance configurés de manière explicite.

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau serveur, sélectionnez le type d'adresse IP (IPv4 ou IPv6), saisissez l'adresse IP du serveur et cliquez sur **OK**.
- Sélectionnez un serveur et cliquez sur **Edit** (Modifier) pour modifier l'adresse.
- Sélectionnez un serveur et cliquez sur **Delete** (Supprimer) pour le supprimer de la liste des serveurs de confiance.

b) Sélectionnez ou désélectionnez les options suivantes :

- **Any** (Tous) : faites confiance à tous les serveurs DNS, surveillez-les tous. Cette option est désactivée par défaut.
- **Configured-Servers** (Serveurs configurés) : indique si les serveurs configurés dans les groupes de serveurs DNS doivent être considérés comme fiables. Par défaut, cette option est activée.

- **DHCP-Client** (Client DHCP) : indique si les serveurs identifiés par la surveillance des messages entre un client DHCP et un serveur DHCP sont considérés comme des serveurs DNS de confiance. Par défaut, cette option est activée.
- **DHCP-Pools** (Ensembles DHCP) : indique si les serveurs DNS configurés dans les ensembles DHCP pour les clients qui obtiennent des adresses par l'intermédiaire des serveurs DHCP exécutés sur les interfaces d'appareils doivent être considérés comme fiables. Par défaut, cette option est activée.
- **DHCP-Relay** (Relais DHCP) : indique si les serveurs identifiés par la surveillance des messages de relais DHCP entre un client DHCP et un serveur DHCP sont considérés comme des serveurs DNS de confiance. Par défaut, cette option est activée.

Étape 7 (Facultatif) Cochez la case **Enable DNS Guard on all interfaces** (Activer la protection DNS sur toutes les interfaces) pour appliquer une réponse DNS par requête.

Vous pouvez également définir la protection DNS lors de la configuration de l'inspection DNS. Pour une interface donnée, le paramètre de protection DNS configuré dans l'inspection DNS a priorité sur ce paramètre global. Par défaut, l'inspection DNS est activée sur toutes les interfaces avec l'option de protection DNS activée.

Étape 8 (Facultatif) Mappez les domaines à des groupes de serveurs DNS spécifiques.

Vous pouvez mapper jusqu'à 30 domaines. Vous ne pouvez pas mapper le même domaine à plusieurs groupes de serveurs DNS, mais vous pouvez mapper plusieurs domaines au même groupe de serveurs. Ne mappez aucun domaine au groupe que vous souhaitez utiliser par défaut (par exemple, DefaultDNS).

a) Dans la zone **DNS Group Map** (Carte de groupe DNS), cochez **Enable DNS Group Map** (Activer la carte de groupe DNS).
b) Cliquez sur **Add** (ajouter).

   La boîte de dialogue **Add Domains to DNS Server Group** (Ajouter des domaines au groupe de serveurs DNS) apparaît.

c) Dans la liste déroulante **DNS server group to domain name mapping** (Mappage du groupe de serveurs DNS au nom de domaine), sélectionnez le nom du groupe de serveurs DNS.
d) Dans le champ **Domain Name** (Nom de domaine), saisissez le nom de domaine que vous souhaitez mapper au groupe DNS.
e) Cliquez sur **OK**.
f) Répétez ces étapes pour ajouter d'autres mappages.

Étape 9 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer le contournement matériel et l'alimentation double (Cisco ISA 3000)

Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Les paires d'interfaces prises en charge sont les interfaces en cuivre GigabitEthernet 1/1 et 1/2; et GigabitEthernet 1/3 et 1/4. Lorsque le contournement matériel est actif, aucune fonction de pare-feu n'est en place. Veuillez donc vous assurer de bien comprendre les risques liés à l'autorisation du trafic de transit. Consultez les lignes directrices suivantes relatives au contournement matériel :

- Cette fonctionnalité est uniquement disponible sur le périphérique Cisco ISA 3000.
- Si vous avez un modèle Ethernet à fibre optique, seule la paire Ethernet en cuivre (GigabitEthernet 1/1 et 1/2) prend en charge le contournement matériel.
- Lorsque l'ISA 3000 perd de l'alimentation et passe en mode de contournement matériel, seules les paires d'interfaces prises en charge peuvent communiquer; avec la configuration par défaut, inside1 <---> inside2 et outside1 <---> outside2 ne peuvent plus communiquer. Toutes les connexions existantes entre ces interfaces seront perdues.
- Nous vous suggérons de désactiver la répartition aléatoire des séquences TCP (comme le décrit cette procédure). Si la répartition aléatoire est activée (par défaut), lorsque le contournement matériel sera activé, les sessions TCP devront être rétablies. Par défaut, l'ISA 3000 réécrit le numéro de séquence initial (ISN) des connexions TCP qui le traversent en nombre aléatoire. Lorsque le contournement matériel est activé, l'ISA 3000 ne se trouve plus dans le chemin de données et ne traduit pas les numéros de séquence; le client destinataire reçoit un numéro de séquence inattendu et interrompt la connexion. Même lorsque la répartition aléatoire de la séquence TCP est désactivée, certaines connexions TCP devront être rétablies car la liaison a été temporairement interrompue pendant le basculement.
- Les connexions Cisco TrustSec sur les interfaces de contournement matériel sont abandonnées lorsque le contournement matériel est activé. Lorsque l'ISA 3000 démarre et que le contournement matériel est désactivé, les connexions sont renégociées.
- Lorsque le contournement matériel est désactivé et que le trafic reprend par le chemin de données de l'ISA 3000, certaines sessions TCP existantes doivent être rétablies en raison de la liaison qui est temporairement inactive pendant le basculement.
- Lorsque le contournement matériel est actif, les PHY Ethernet sont déconnectés, de sorte que l'ASA ne peut pas déterminer l'état de l'interface. Les interfaces peuvent sembler être en panne.

Pour les alimentations doubles dans l'ISA 3000, vous pouvez établir des alimentations doubles comme la configuration attendue dans le système d'exploitation ASA. En cas de défaillance d'une alimentation, l'ASA émet une alarme. Par défaut, l'ASA s'attend à une seule alimentation et n'émettra pas d'alarme tant qu'il dispose d'une alimentation opérationnelle.

Avant de commencer

- Vous devez connecter les interfaces de contournement matériel pour accéder aux ports du commutateur. Ne les connectez pas aux ports de ligne principale.

Procédure

Étape 1 Pour configurer le contournement matériel, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Hardware Bypass (Contournement matériel)**.

Étape 2 Configurez le contournement matériel pour qu'il s'active pour chaque paire d'interfaces en cochant la case **Enable Bypass during Power Down** (Activer le contournement pendant une panne de courant).

Étape 3 (Facultatif) Configurez chaque paire d'interfaces pour qu'elle reste en mode de contournement matériel après le rétablissement du courant et le démarrage du périphérique en cochant la case **Stay in Bypass after Power Up (Rester en contournement après le redémarrage)**.

Lorsque le contournement matériel est désactivé, il y a une brève interruption de la connexion lorsque l'ASA prend en charge les flux. Dans ce cas, vous devez désactiver manuellement le contournement matériel lorsque vous êtes prêt; cette option vous permet de contrôler le moment où une brève interruption se produit.

Étape 4 Pour une paire d'interfaces, activez ou désactivez manuellement le contournement matériel en cochant la case **Bypass Immediately** (Contourner immédiatement).

Étape 5 (Facultatif) Configurez le contournement matériel pour qu'il reste actif jusqu'après le démarrage du module ASA FirePOWER en cochant la case **Stay in Bypass Mode until after the ASA Firepower Module Boots Up** (Rester en mode de contournement jusqu'après le démarrage du module ASA Firepower).

Vous devez activer le contournement matériel sans l'option **Stay in Bypass after Power Up** (Rester en contournement après le redémarrage) pour que le délai de démarrage fonctionne. Sans cette option, le contournement matériel risque de devenir inactif avant la fin du démarrage du module ASA FirePOWER. Ce scénario peut entraîner l'abandon du trafic si vous avez configuré le module en cas de non-conformité, par exemple.

Étape 6 Cliquez sur **Apply** (Appliquer).

Étape 7 Désactivez la répartition aléatoire de la séquence TCP. Cet exemple montre comment désactiver la répartition aléatoire pour tout le trafic en ajoutant le paramètre à la configuration par défaut.

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy (Politique de service)**.
b) Sélectionnez la règle **sfrclass** et cliquez sur **Edit** (Modifier).
c) Cliquez sur **Rule Actions** (Actions de règles), puis sur **Connection Settings** (Paramètres de connexion).
d) Décochez la case **Randomize Sequence Number** (Numéro de séquence aléatoire).
e) Cliquez sur **OK**, puis sur **Apply**(appliquer).

Étape 8 Pour établir les alimentations doubles comme configuration attendue, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Power Supply (Alimentation)**, cochez la case **Enable Redundant Power Supply** (Activer l'alimentation redondante), puis cliquez sur **Apply** (Appliquer).

Cet écran affiche également les alimentations disponibles.

Étape 9 Cliquez sur **Save** (Enregistrer).

Le comportement du contournement matériel après la mise en ligne du système est déterminé par les paramètres de configuration dans la configuration de démarrage. Vous devez donc enregistrer votre configuration en cours d'exécution.

Modifier les performances et le comportement ASP (Accelerated Security Path)

L'ASP est une couche d'implémentation qui met en œuvre vos politiques et vos configurations. Elle ne présente pas d'intérêt direct, sauf lors de la résolution de problèmes avec le centre d'assistance technique Cisco. Cependant, il existe certains comportements liés aux performances et à la fiabilité que vous pouvez ajuster.

Choisir un modèle de validation transactionnelle de moteur de règles

Par défaut, lorsque vous modifiez une politique basée sur des règles (comme des critères d'accès), les modifications prennent effet immédiatement. Cependant, cette immédiateté s'accompagne d'une légère perte

de performances. Cette perte de performances est plus notable pour les très grandes listes de règles dans un environnement à haut débit de connexions par seconde, par exemple lorsque vous modifiez une stratégie comportant 25 000 règles alors que l'ASA traite 18 000 connexions par seconde.

Les performances sont affectées, car le moteur de règles compile des règles pour accélérer la recherche de règles. Par défaut, le système recherche également les règles non compilées lors de l'évaluation d'une tentative de connexion afin que de nouvelles règles puissent être appliquée; comme les règles ne sont pas compilées, la recherche prend plus de temps.

Vous pouvez modifier ce comportement pour que le moteur de règles utilise un modèle transactionnel lors de la mise en œuvre des modifications de règles, en continuant à utiliser les anciennes règles jusqu'à ce que les nouvelles règles soient compilées et prêtes à l'emploi. Avec le modèle transactionnel, les performances ne devraient pas baisser pendant la compilation des règles. Le tableau suivant clarifie la différence de comportement.

Modèle	Avant la compilation	Pendant la compilation	Après la compilation
Par défaut	Correspond aux anciennes règles.	Correspondance avec les nouvelles règles. (Le débit de connexions par seconde diminue.)	Correspond aux nouvelles règles.
Transactionnel	Correspond aux anciennes règles.	Correspondance avec les anciennes règles. (Le débit de connexions par seconde n'est pas affecté.)	Correspond aux nouvelles règles.

Un avantage supplémentaire du modèle transactionnel est que, lors du remplacement d'une ACL sur une interface, il n'y a aucun intervalle entre la suppression de l'ancienne ACL et l'application de la nouvelle. Cette fonctionnalité réduit le risque que des connexions acceptables soient abandonnées pendant l'opération.

Avant de commencer

- La validation transactionnelle n'est pas conseillée pour les règles de contrôle d'accès si vous utilisez des objets FQDN pour des noms d'hôte dont la résolution peut changer fréquemment, car la compilation du groupe d'accès pourrait ne jamais aboutir complètement en raison des fluctuations DNS. Si vous souhaitez tout de même utiliser la validation transactionnelle, envisagez d'allonger le délai d'expiration du DNS.
- Si vous activez le modèle transactionnel pour un type de règle, des journaux système marquant le début et la fin de la compilation sont générés. Ces journaux système sont numérotés de 780 001 à 780 004.

Procédure

Choisissez **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Rule Engine (Moteur de règles)** et sélectionnez les options souhaitées :

- **Groupe d'accès** : critères d'accès appliqués globalement ou aux interfaces.
- **NAT** : règles de traduction des adresses réseau.

Activer l'équilibrage de charges ASP

Le mécanisme d'équilibrage de charges ASP permet d'éviter les problèmes suivants :

- Dépassements causés par des pics de trafic imprévus sur les flux
- Dépassements causés par des flux volumineux surchargeant les anneaux de réception d'interfaces spécifiques
- Dépassements causés par des anneaux de réception d'interfaces relativement surchargés, dans lesquels un seul cœur ne peut pas supporter la charge.

L'équilibrage de charges ASP permet à plusieurs cœurs de travailler simultanément sur les paquets qui ont été reçus d'un seul anneau de réception d'interface. Si le système abandonne des paquets et que la sortie de la commande **show cpu** est bien inférieure à 100 %, cette fonctionnalité peut améliorer votre débit si les paquets appartiennent à de nombreuses connexions non liées.



Remarque L'équilibrage de charges ASP est désactivé sur l'ASA virtuel. Avec l'intégration de DPDK (Dataplane Development Kit) dans le chemin de sécurité accéléré (ASP) de l'ASA virtuel, l'ASA virtuel affiche de meilleures performances avec cette fonctionnalité désactivée.

Procédure

Étape 1 Pour activer et désactiver automatiquement l'équilibrage de charges ASP, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **ASP Load Balancing (Équilibrage de charges ASP)** et cochez la case **Dynamically enable or disable ASP load balancing based on traffic monitoring** (Activer ou désactiver dynamiquement l'équilibrage de charges ASP en fonction de la supervision du trafic).

Étape 2 Pour activer ou désactiver manuellement l'équilibrage de charges ASP, cochez ou décochez la case **Enable ASP load balancing** (Activer l'équilibrage de charges ASP).

Lorsque vous activez manuellement l'équilibrage de charges ASP, il est activé jusqu'à ce que vous le désactiviez manuellement, même si l'option Dynamic (Dynamique) est également activée. La désactivation manuelle de l'équilibrage de charges ASP s'applique uniquement si vous avez activé manuellement l'équilibrage de charges ASP. Si vous avez également activé l'option Dynamic (Dynamique), le système revient à l'activation ou à la désactivation automatique de l'équilibrage de charges ASP.

Supervision du cache DNS

L'ASA fournit un cache local des renseignements DNS à partir des demandes DNS externes qui sont envoyées pour certaines commandes de VPN et de certificat SSL VPN sans client. Chaque demande de traduction DNS est d'abord recherchée dans le cache local. Si la mémoire cache locale contient les informations, l'adresse IP qui en résulte est renvoyée. Si la mémoire cache locale ne peut pas résoudre la demande, une requête DNS

est envoyée aux différents serveurs DNS qui ont été configurés. Si un serveur DNS externe résout la demande, l'adresse IP qui en résulte est stockée dans la mémoire cache locale avec son nom d'hôte correspondant.

Consultez la commande suivante pour superviser le cache DNS :

- **show dns-hosts**

  Cette commande affiche le cache DNS, qui comprend les entrées apprises dynamiquement à partir d'un serveur DNS ainsi que le nom et les adresses IP saisis manuellement à l'aide de la commande name.

Historique des paramètres de base

Nom de la caractéristique	Versions de plateforme	Description
Plusieurs groupes de serveurs DNS	9.18(1)	Vous pouvez désormais utiliser plusieurs groupes de serveurs DNS : un groupe est le groupe par défaut, tandis que les autres groupes peuvent être associés à des domaines spécifiques. Une requête DNS qui correspond à un domaine associé à un groupe de serveurs DNS utilisera ce groupe. Par exemple, si vous souhaitez que le trafic destiné aux serveurs internes eng.cisco.com utilise un serveur DNS interne, vous pouvez mapper eng.cisco.com à un groupe DNS interne. Toutes les requêtes DNS qui ne correspondent pas à un mappage de domaine utiliseront le groupe de serveurs DNS par défaut, qui n'a pas de domaine associé. Par exemple, le groupe DefaultDNS peut inclure un serveur DNS public disponible sur l'interface externe. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**
Serveurs DNS de confiance pour la résolution du domaine d'objet de service réseau.	9.17(1)	Vous pouvez spécifier les serveurs DNS auxquels le système doit faire confiance lors de la résolution des noms de domaine dans les objets de service de réseau. Cette fonctionnalité garantit que toutes les résolutions de noms de domaine DNS acquièrent des adresses IP auprès de sources de confiance. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**
Modification du comportement de la TTL de l'entrée DNS	9.17(1)	Auparavant, la valeur configurée était ajoutée à la TTL existante de chaque entrée (la valeur par défaut était de 1 minute). Désormais, si le délai d'expiration est plus long que la TTL de l'entrée, cette dernière est augmentée jusqu'à la valeur du délai d'expiration de l'entrée. Si la TTL est plus longue que le délai d'expiration, la valeur du délai d'expiration est ignorée; dans ce cas, aucun délai supplémentaire n'est ajouté à la TTL. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)** > **Configure multiple DNS server groups (Configurer plusieurs groupes de serveurs DNS)**

Nom de la caractéristique	Versions de plateforme	Description
Exigences relatives à l'utilisateur local et au mot de passe d'activation	9.17(1)	Pour les utilisateurs locaux et le mot de passe d'activation, les exigences de mot de passe suivantes ont été ajoutées : • Longueur du mot de passe : au moins 8 caractères. Auparavant, le minimum était de 3 caractères. • Caractères répétitifs et séquentiels : trois caractères ASCII ou plus consécutifs ne sont pas autorisés. Par exemple, les mots de passe suivants seront refusés : • **abc**utilisateur1 • utilisateur**543** • utilisateur**aaaa** • utilisateur2**666** Écrans Nouveaux ou modifiés : • **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)**
Prise en charge NTPv4	9.14(1)	L'ASA prend désormais en charge NTPv4. Aucun écran modifié.
Algorithmes d'authentification NTP supplémentaires	9.13(1)	Auparavant, seul MD5 était pris en charge pour l'authentification NTP. L'ASA prend désormais en charge les algorithmes suivants : • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC Écrans Nouveaux ou modifiés : **Configuration** > **Device Setup (Configuration de l'appareil)** > **System Time (Heure du système)** > **NTP** > **bouton Add (Ajouter) > boîte de dialogue Add NTP Server Configuration (Ajouter une configuration de serveur NTP) > liste déroulante Key Algorithm (Algorithme de clé)**

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de NTP sur IPv6	9.12(1)	Vous pouvez maintenant spécifier une adresse IPv6 pour le serveur NTP. Écrans Nouveaux ou modifiés : **Configuration** > **Device Setup (Configuration de l'appareil)** > **System Time (Heure du système)** > **NTP** > **bouton Add (Ajouter) > boîte de dialogue Add NTP Server Configuration (Ajouter une configuration de serveur NTP)**
Le changement de mot de passe **enable** est maintenant requis lors de la connexion	9.12(1)	Le mot de passe par défaut **enable** est vide. Lorsque vous essayez d'accéder en mode d'exécution privilégié sur l'ASA, vous devez désormais modifier le mot de passe pour une valeur de 3 à 127 caractères. Vous ne pouvez pas le garder vide. La commande **no enable password** n'est plus prise en charge. Au niveau de l'interface de ligne de commande, vous pouvez accéder au mode d'exécution privilégié à l'aide des commandes **enable**, **login** (avec un utilisateur de niveau de privilège 2+), ou d'une session SSH ou Telnet lorsque vous activez **aaa authorization exec auto-enable**. Toutes ces méthodes nécessitent que vous définissiez le mot de passe d'activation. Cette exigence de changement de mot de passe n'est pas appliquée pour les connexions ASDM. Dans ASDM, par défaut, vous pouvez vous connecter sans nom d'utilisateur et avec le mot de passe **enable**. Aucun écran modifié.
L'équilibrage de charges ASP est désactivé sur l'ASA virtuel	9.10(1)	Avec la récente intégration de DPDK (Dataplane Development Kit) dans le chemin de sécurité accéléré (ASP) de l'ASA virtuel, l'ASA virtuel affiche de meilleures performances avec cette fonctionnalité désactivée.
L'équilibrage automatique de la charge ASP est désormais pris en charge pour l'ASA virtuel.	9.8(1)	Auparavant, vous pouviez uniquement activer et désactiver manuellement l'équilibrage de charges ASP. Nous avons modifié l'écran suivant : **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > ASP Load Balancing (Équilibrage de charges ASP)**
Hachage PBKDF2 pour tous les mots de passe locaux **username** et **enable**	9.7(1)	Les mots de passe locaux **username** et **enable** de toutes les longueurs sont stockés dans la configuration à l'aide du hachage PBKDF2 (Password-Based Key Derivation Function 2) à l'aide de SHA-512. Auparavant, les mots de passe de 32 caractères et moins utilisaient la méthode de hachage basée sur MD5. Les mots de passe existants continuent d'utiliser le hachage basé sur MD5, sauf si vous entrez un nouveau mot de passe. Consultez le chapitre « Logiciels et configurations » du Guide de configuration des opérations générales pour connaître les lignes directrices relatives à la rétrogradation. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)** > **Enable Password (Mot de passe d'activation)** **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)** > **Identity (Identité)**

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge des alimentations doubles pour l'ISA 3000	9.6(1)	Pour les alimentations doubles dans l'ISA 3000, vous pouvez établir des alimentations doubles comme la configuration attendue dans le système d'exploitation ASA. En cas de défaillance d'une alimentation, l'ASA émet une alarme. Par défaut, l'ASA s'attend à une seule alimentation et n'émettra pas d'alarme tant qu'il dispose d'une alimentation opérationnelle. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Power Supply (Alimentation)**
Prise en charge de mots de passe plus longs pour les mots de passe locaux **username** et **enable** (jusqu'à 127 caractères)	9.6(1)	Vous pouvez désormais créer des mots de passe **username** et **enable** locaux jusqu'à 127 caractères (l'ancienne limite était de 32). Lorsque vous créez un mot de passe de plus de 32 caractères, il est stocké dans la configuration à l'aide d'un hachage PBCDF2 (Password-Based Key Derivation Function 2). Les mots de passe plus courts continuent d'utiliser la méthode de hachage basée sur MD5. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)** > **Enable Password (Mot de passe d'activation)** **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)** > **Identity (Identité)**
contournement matériel ISA 3000	9.4(1.225)	L'ISA 3000 prend en charge une fonction de contournement matériel pour permettre au trafic de continuer à circuler dans l'appareil en cas de perte d'alimentation. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Hardware Bypass (Contournement matériel)** *Cette fonctionnalité n'est pas disponible dans la version 9.5(1).*
Équilibrage de charges ASP automatique	9.3(2)	Vous pouvez maintenant activer le basculement automatique vers la fonction d'équilibrage de charges ASP. **Remarque** La fonction automatique n'est pas prise en charge sur l'ASA virtuel; seules l'activation et la désactivation manuelles sont prises en charge. Nous avons modifié l'écran suivant : **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > ASP Load Balancing (Équilibrage de charges ASP)**

Nom de la caractéristique	Versions de plateforme	Description
Suppression du mot de passe Telnet par défaut	9.0(2)/9.1(2)	Pour améliorer la sécurité de l'accès de gestion à l'ASA, le mot de passe de connexion par défaut pour Telnet a été supprimé; vous devez définir manuellement le mot de passe avant de pouvoir vous connecter en utilisant Telnet. **Remarque** Le mot de passe de connexion n'est utilisé pour Telnet que si vous ne configurez pas l'authentification de l'utilisateur Telnet. Auparavant, lorsque vous effaciez le mot de passe, l'ASA rétablissait le mot de passe par défaut « cisco ». Maintenant, lorsque vous effacez le mot de passe, le mot de passe est supprimé. Le mot de passe de connexion est également utilisé pour les sessions Telnet, du commutateur à l'ASASM (voir la commande **session**). Pour l'accès initial à l'ASASM, vous devez utiliser la commande **service-module session**, jusqu'à ce que vous définissiez un mot de passe de connexion. Nous n'avons pas modifié d'écrans ASDM.
Visibilité du chiffrement des mots de passe	v 8.4(1)	Nous avons modifié la commande **show password encryption**.
Phrase secrète principale	8.3(1)	Nous avons introduit cette fonctionnalité. La phrase secrète principale vous permet de stocker en toute sécurité les mots de passe en texte brut dans un format chiffré et fournit une clé utilisée pour chiffrer ou masquer tous les mots de passe de manière universelle, sans modifier aucune fonctionnalité. Nous avons introduit les écrans suivants : **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Master Passphrase (Phrase secrète principale)** **Configuration > Device Management (Gestion des périphériques) > Device Administration (Administration des périphériques) > Master Passphrase (Phrase secrète principale)**



CHAPITRE 25

Services DHCP et DDNS

Ce chapitre décrit comment configurer le serveur DHCP ou le relais DHCP, ainsi que les méthodes de mise à jour du DNS dynamique (DDNS).

- À propos des services DHCP et DDNS, à la page 781
- Lignes directrices pour les services DHCP et DDNS, à la page 784
- Configurer le serveur DHCP, à la page 786
- Configurer les agents de relais DHCP., à la page 791
- Configuration du DNS dynamique, à la page 792
- Supervision des services DHCP et DDNS, à la page 797
- Historique des services DHCP et DDNS, à la page 799

À propos des services DHCP et DDNS

Ce sujet décrit le serveur DHCP, l'agent de relais DHCP et la mise à jour DDNS.

Serveur DHCPv4

Un serveur DHCP fournit des paramètres de configuration réseau, tels que des adresses IP, aux clients DHCP.

- fournit les paramètres de configuration directement aux clients DHCP connectés aux interfaces ASA, et
- utilise la communication par port UDP pour les messages client-serveur.

Détails de la communication du serveur DHCPv4

La communication DHCP utilise des protocoles réseau et des affectations de port spécifiques :

- Client DHCP IPv4 : utilise l'adresse de diffusion plutôt que de multidiffusion pour atteindre le serveur et est à l'écoute des messages sur le port UDP 68
- Le serveur DHCP écoute les messages sur le port UDP 67.

Options de DHCP

DHCP fournit une structure pour la transmission des informations de configuration aux hôtes sur un réseau TCP/IP. Les paramètres de configuration sont transportés dans des éléments étiquetés qui sont stockés dans le champ Options du message DHCP. Les données sont également appelées options. Les renseignements sur

le fournisseur sont également stockés dans Options, et tous les postes d'informations sur le fournisseur peuvent être utilisés comme options DHCP.

Options DHCP courantes

Les téléphones IP Cisco téléchargent leur configuration à partir d'un serveur TFTP. Lorsqu'un téléphone IP Cisco démarre, si l'adresse IP et l'adresse IP du serveur TFTP ne sont pas préconfigurées, il envoie une demande avec l'option 150 ou 66 au serveur DHCP pour obtenir cette information.

- L'option 150 de DHCP fournit les adresses IP d'une liste de serveurs TFTP.
- L'option DHCP 66 fournit l'adresse IP ou le nom d'hôte d'un seul serveur TFTP.
- L'option 3 de DHCP définit la voie de routage par défaut.

Une seule demande peut inclure les deux options 150 et 66. Dans ce cas, le serveur DHCP fournit des valeurs pour les deux options dans la réponse si elles sont déjà configurées sur l'ASA.

Vous pouvez utiliser les options DHCP avancées pour fournir les paramètres DNS, WINS et de nom de domaine aux clients DHCP. L'option DHCP 15 est utilisée pour le suffixe de domaine DNS. Vous pouvez également utiliser le paramètre de configuration automatique DHCP pour obtenir ces valeurs ou les définir manuellement. Lorsque vous utilisez plusieurs méthodes pour définir ces informations, elles sont transmises aux clients DHCP dans l'ordre suivant :

1. Paramètres configurés manuellement.
2. Paramètres des options DHCP avancées
3. Paramètres de configuration automatique de DHCP.

Priorité de configuration du nom de domaine

Vous pouvez définir manuellement le nom de domaine que vous souhaitez que les clients DHCP reçoivent, puis activer la configuration automatique de DHCP. Bien que la configuration automatique de DHCP découvre le domaine ainsi que les serveurs DNS et WINS, le nom de domaine défini manuellement est transmis aux clients DHCP avec les noms de serveurs DNS et WINS découverts, car le nom de domaine découvert par le processus de configuration automatique de DHCP est remplacé par l' domaine défini.

Serveur sans état DHCPv6

Un serveur DHCPv6 sans état est une configuration DHCP IPv6 qui

- fournit des informations telles que le serveur DNS ou le nom de domaine lorsque les clients envoient des paquets de demande d'information (IR),
- accepte les paquets IR, mais n'affecte pas d'adresse aux clients, et
- fonctionne en conjonction avec les fonctionnalités de configuration automatique d'adresse sans état (SLAAC) et de délégation de préfixe.

Fonctionnement du serveur DHCPv6 sans état

Pour les clients qui utilisent la configuration automatique des adresses sans état (SLAAC) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6, à la page 711), vous pouvez configurer les ASA pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que ASA a reçu à l'aide de la délégation de préfixe.

Agents de relais DHCP

Un agent de relais DHCP transfère les demandes DHCP reçues sur une interface vers un ou plusieurs serveurs DHCP.

Opération de l'agent de relais DHCP

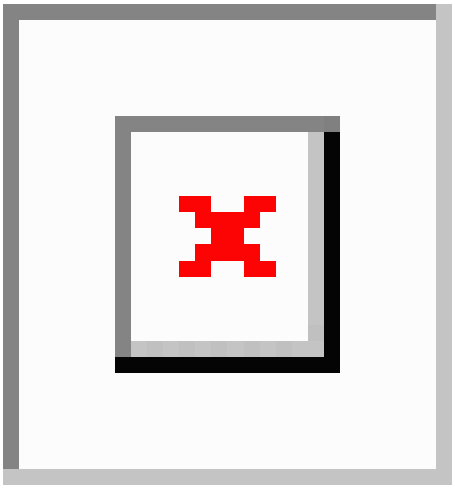
Les clients DHCP utilisent les diffusions UDP pour envoyer leurs premiers messages DHCPDISCOVER, car ils ne disposent pas d'informations sur le réseau auquel ils sont connectés. Si le client se trouve sur un segment de réseau qui n'inclut pas de serveur, les diffusions UDP ne sont normalement pas transférées par le périphérique ASA, car il ne transfère pas le trafic de diffusion. L'agent de relais DHCP vous permet de configurer l'interface de l'ASA qui reçoit les diffusions pour transférer les demandes DHCP vers un serveur DHCP qui est disponible via un autre périphérique.

Prise en charge du serveur relais DHCP sur VTI

Vous pouvez configurer un agent de relais DHCP sur une interface ASA pour recevoir et transférer des messages DHCP entre un client DHCP et un serveur DHCP. Cependant, un serveur de relais DHCP pour transférer des messages par l'intermédiaire d'une interface logique n'était pas pris en charge.

La figure suivante montre le processus de découverte du client DHCP et du serveur DHCP qui utilise le relais DHCP sur le VPN VTI. L'agent de relais DHCP, configuré sur l'interface VTI du site 1 de l'ASA, reçoit le paquet DHCPDISCOVER du client DHCP et envoie le paquet par le tunnel VTI. Le site 2 de l'ASA transmet le paquet DHCPDISCOVER au serveur DHCP. Le serveur DHCP répond par un DHCPOFFER au site 2 de l'ASA. L'ASA du site 2 l'envoie au relais DHCP (site 1 de l'ASA), qui l'envoie au client DHCP.

Illustration 79 : Serveur relais DHCP sur VTI



La même procédure est suivie pour les exigences DHCPREQUEST et DHCPACK/NACK.

Lignes directrices pour les services DHCP et DDNS

Restrictions en mode contexte

Le serveur sans état DHCPv6 n'est pas pris en charge en mode contexte multiple.

Restrictions en mode de pare-feu

Tenez compte de ces limites du mode de pare-feu lors de la configuration des services DHCP et DDNS :

- Le relais DHCP n'est pas pris en charge en mode transparent de pare-feu ou en mode routé sur l'interface de BVI ou l'interface de membre du groupe de ponts.
- Le serveur DHCP est pris en charge en mode de pare-feu transparent sur une interface de membre de groupe de ponts. En mode routé, le serveur DHCP est pris en charge sur l'interface BVI, pas sur l'interface des membres du groupe de ponts. Les BVI doivent avoir un nom pour que le serveur DHCP puisse fonctionner.
- DDNS n'est pas pris en charge en mode de pare -feu transparent ou en mode routé sur l'interface de BVI ou l'interface de membre du groupe de ponts.
- Le serveur sans état DHCPv6 n'est pas pris en charge en mode de pare-feu transparent ou en mode routé sur l'interface de BVI ou de membre du groupe de ponts.

Limites de la mise en grappe

Le serveur sans état DHCPv6 n'est pas pris en charge par la mise en grappe.

Prise en charge d'IPv6

Lignes directrices relatives au serveur DHCPv4

Suivez ces lignes directrices lors de la configuration du serveur DHCPv4 :

- L'ensemble DHCP disponible maximal est de 256 adresses.

- Vous pouvez configurer un serveur DHCP sur n'importe quelle interface avec un nom et une adresse IP, comme une interface physique, une sous-interface ou une BVI en mode routé.
- Ne sélectionnez pas une interface qui utilise DHCP ou PPPoE pour obtenir son adresse en tant qu'interface de serveur DHCP.
- Vous ne pouvez configurer qu'un seul serveur DHCP sur chaque interface. Chaque interface peut avoir son propre ensemble d'adresses à utiliser. Cependant, les autres paramètres DHCP, tels que les serveurs DNS, le nom de domaine, les options, le délai de ping et les serveurs WINS, sont configurés globalement et utilisés par le serveur DHCP sur toutes les interfaces.
- Vous ne pouvez pas configurer une interface en tant que client DHCP si un serveur DHCP est également activé sur cette interface; vous devez utiliser une adresse IP statique.
- Vous ne pouvez pas configurer un serveur DHCP et un relais DHCP sur le même périphérique, même si vous souhaitez les activer sur des interfaces différentes; vous ne pouvez configurer qu'un seul type de service.
- Vous pouvez réserver une adresse DHCP pour une interface. ASA attribue une adresse spécifique de l'ensemble d'adresses à un client DHCP en fonction de l'adresse MAC du client.
- L'ASA ne prend pas en charge les clients DHCP derrière les serveurs de relais DHCP; le client doit être connecté directement à ASA.
- Le serveur DHCP ne prend pas en charge les demandes BOOTP.

Lignes directrices relatives au serveur DHCPv6

Tenez compte de ces lignes directrices lors de la configuration du serveur DHCPv6 :

- Le serveur sans état DHCPv6 ne peut pas être configuré sur une interface où l'adresse DHCPv6, le client de délégation de préfixe ou le relais DHCPv6 est configuré.

Lignes directrices relatives au relais DHCP

Suivez ces lignes directrices lors de la configuration du relais DHCP :

- Vous pouvez configurer un maximum de 10 serveurs relais DHCPv4, avec un maximum de 4 serveurs par interface.
- Vous pouvez configurer un maximum de 10 serveurs relais DHCPv6. Les serveurs propres à une interface pour IPv6 ne sont pas pris en charge.
- Vous ne pouvez pas configurer un serveur DHCP et un relais DHCP sur le même périphérique, même si vous souhaitez les activer sur des interfaces différentes; vous ne pouvez configurer qu'un seul type de service.
- Ne sélectionnez pas une interface qui utilise DHCP ou PPPoE pour obtenir son adresse en tant qu'interface de relais DHCP.
- Les services de relais DHCP ne sont pas offerts dans le mode transparent du pare-feu ou le mode routé sur l'interface des BVI ou celle des membres du groupe de ponts. Vous pouvez, cependant, autoriser le trafic DHCP en utilisant une règle d'accès. Pour autoriser les demandes et les réponses DHCP par l'intermédiaire de l'ASA, vous devez configurer deux règles d'accès, une qui autorise les demandes DHCP de l'interface interne vers l'extérieur (port de destination d'UDP 67) et une qui autorise les réponses du serveur de l'autre côté (port de destination UDP 68).

- Pour IPv4, les clients doivent être connectés directement à ASA et ne peuvent pas envoyer de demandes par un autre agent de relais ou un routeur. Pour IPv6, ASA prend en charge les paquets d'un autre serveur de relais.
- Les clients DHCP doivent se trouver sur des interfaces différentes des serveurs DHCP vers lesquels ASA relaye les demandes.
- Vous ne pouvez pas activer le relais DHCP sur une interface dans une zone de trafic.

Configuration du service DDNS

Le DDNS du pare-feu prend uniquement en charge le service DynDNS. Par conséquent, assurez-vous que le DDNS est configuré avec l'URL de mise à jour dans la syntaxe suivante :

https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**.

Configurer le serveur DHCP

Cette section décrit comment configurer un serveur DHCP fourni par l'ASA.

Procédure

Étape 1 Activer le serveur DHCPv4, à la page 786.
Étape 2 Configurer les options DHCPv4 avancées, à la page 788.
Étape 3 Configurer le serveur sans état DHCPv6, à la page 789.

Activer le serveur DHCPv4

Pour activer le serveur DHCP sur une interface ASA, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Server (Serveur DHCP)**.

Étape 2 Choisissez une interface, puis cliquez sur **Edit** (Modifier).

En mode transparent, choisissez une interface de membres de groupe de ponts. En mode routé, choisissez une interface routée ou un BVI; ne choisissez pas l'interface des membres du groupe de ponts.

a) Cochez la case **Enable DHCP Server** (Activer le serveur DHCP) pour activer le serveur DHCP sur l'interface sélectionnée.
b) Dans le champ **DHCP Address Pool** (Ensemble d'adresses DHCP), saisissez la plage d'adresses IP (de la plus basse à la plus élevée) qu'utilise le serveur DHCP. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et elle ne peut pas inclure l'adresse IP de l'interface elle-même.

c) Définissez les éléments suivants dans le champ **Optional Parameters** (Paramètres facultatifs) :

- Les serveurs DNS (1 et 2) configurés pour l'interface.
- Les serveurs WINS (principaux et secondaires) configurés pour l'interface.
- Le nom de domaine de l'interface.
- Le temps en millisecondes pendant lequel l'ASA attendra une réponse après l'envoi d'un message Ping ICMP sur l'interface.
- La durée pendant laquelle le serveur DHCP configuré sur l'interface permet aux clients DHCP d'utiliser une adresse IP attribuée.
- L'interface d'un client DHCP qui fournit des renseignements sur le DNS, le WINS et le nom de domaine pour la configuration automatique si l'ASA agit en tant que client DHCP sur une interface spécifiée (généralement à l'extérieur).
- Cliquez sur **Advanced** (Avancé) pour afficher la boîte de dialogue **Advanced DHCP Options** (Options DHCP avancées) afin de configurer d'autres options DHCP. Consultez Configurer les options DHCPv4 avancées, à la page 788 pour de plus amples renseignements.

d) Cochez la case **Update DNS Clients** (Mettre à jour les clients DNS) dans la zone **Dynamic Settings for DHCP Server** (Paramètres dynamiques pour le serveur DHCP) pour préciser qu'en plus de l'action par défaut de mise à jour des enregistrements de ressources PTR des clients, le serveur DHCP sélectionné doit également effectuer les actions de mise à jour suivantes :

- Cochez la case **Update Both Records** (Mettre à jour les deux enregistrements) pour préciser que le serveur DHCP doit mettre à jour les RR A et PTR.
- Cochez la case **Override Client Settings** (Remplacer les paramètres du client) pour préciser que les actions du serveur DHCP doivent remplacer toutes les actions de mise à jour demandées par le client DHCP.

e) Cliquez sur **OK** pour fermer la boîte de dialogue **Edit DHCP Server** (Modifier le serveur DHCP).

Étape 3 (Facultatif) (Mode routé) Cochez la case **Enable Auto-configuration from interface** (Activer la configuration automatique de l'interface) dans la zone **Global DHCP Options** (Options DHCP globales) sous le tableau des serveurs DHCP pour activer la configuration automatique DHCP uniquement si l'ASA agit en tant que client DHCP sur une interface spécifiée (généralement à l'extérieur).

La configuration automatique DHCP permet au serveur DHCP de fournir aux clients DHCP des informations sur le serveur DNS, le nom de domaine et le serveur WINS obtenues d'un client DHCP qui s'exécute sur l'interface précisée. Si les renseignements obtenus par la configuration automatique sont également spécifiés manuellement dans la zone **Global DHCP Options** (Options DHCP globales), les renseignements spécifiés manuellement prévalent sur les renseignements découverts.

Étape 4 Choisissez l'interface de configuation automatique dans la liste déroulante.

Étape 5 Cochez la case **Allow VPN override** (Autoriser le remplacement du VPN) pour remplacer le paramètre WINS du client DHCP ou PPPoE de l'interface par le paramètre client VPN.

Étape 6 Saisissez l'adresse IP du serveur DNS principal pour un client DHCP dans le champ **DNS Server 1** (Serveur DNS 1).

Étape 7 Saisissez l'adresse IP de l'autre serveur DNS pour un client DHCP dans le champ **DNS Server 2** (Serveur DNS 2).

Étape 8 Saisissez le nom de domaine DNS pour les clients DHCP (par exemple, exemple.com) dans le champ **Domain Name** (Nom de domaine).

Étape 9 Dans le champ **Lease Length** (Durée du bail locatif), saisissez la durée en secondes pendant laquelle le client peut utiliser l'adresse IP qui lui a été attribuée avant l'expiration du bail. Les valeurs valides vont de 300 à 1 048 575 secondes. La valeur par défaut est de 3600 secondes (1 heure).

Étape 10 Saisissez l'adresse IP du serveur WINS principal pour un client DHCP dans le champ **Primary WINS Server** (Serveur WINS principal).

Étape 11 Saisissez l'adresse IP de l'autre serveur WINS pour un client DHCP dans le champ **Secondary WINS Server** (Serveur WINS secondaire).

Étape 12 Pour éviter les conflits d'adresses, l'ASA envoie deux paquets Ping ICMP à une adresse avant d'attribuer cette adresse à un client DHCP. Saisissez la durée, en millisecondes, dans le champ **Ping Timeout** (Délai d'expiration du Ping) pendant laquelle l'ASA attend avant de mettre fin à une tentative de ping DHCP. Les valeurs valides vont de 10 à 10000 millisecondes. La valeur par défaut est de 50 millisecondes.

Étape 13 Cliquez sur **Advanced** (Avancé) pour afficher la boîte de dialogue **Configuring Advanced DHCP Options** (Configuration des options DHCP avancées) afin de spécifier des options DHCP supplémentaires et leurs paramètres. Pour en savoir plus, consultez Configurer les options DHCPv4 avancées, à la page 788.

Étape 14 Vous configurez les paramètres de mise à jour DDNS pour le serveur DHCP dans la zone **Dynamic DNS Settings for DHCP Server** (Paramètres DNS dynamiques pour le serveur DHCP). Cochez la case **Update DNS Clients** (Mettre à jour les clients DNS) pour préciser qu'en plus de l'action par défaut de mise à jour des enregistrements de ressources PTR des clients, le serveur DHCP sélectionné doit également effectuer les actions de mise à jour suivantes :

- Cochez la case **Update Both Records** (Mettre à jour les deux enregistrements) pour préciser que le serveur DHCP doit mettre à jour les RR A et PTR.
- Cochez la case **Override Client Settings** (Remplacer les paramètres du client) pour préciser que les actions du serveur DHCP doivent remplacer toutes les actions de mise à jour demandées par le client DHCP.

Étape 15 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer les options DHCPv4 avancées

L'ASA prend en charge les options DHCP répertoriées dans RFC 2132, RFC 2562 et RFC 5510 pour l'envoi de renseignements. Toutes les options DHCP (1 à 255) sont prises en charge, à l'exception des 1, 12, 50 à 54,58 à 59, 61, 67 et 82.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Server (Serveur DHCP)**, puis cliquez sur **Advanced** (Avancé).

Étape 2 Choisissez le code de l'option dans la liste déroulante.

Étape 3 Choisissez les options que vous souhaitez configurer. Certaines options sont standard. Pour les options standard, le nom de l'option est affiché entre parenthèses après le numéro de l'option et les paramètres de l'option se limitent à ceux pris en charge par l'option. Pour toutes les autres options, seul le numéro d'option s'affiche et vous devez choisir les paramètres appropriés pour fournir l'option. Par exemple, si vous choisissez l'option

DHCP 2 (décalage horaire), vous ne pouvez saisir qu'une valeur hexadécimale pour l'option. Pour toutes les autres options DHCP, tous les types de valeurs d'options sont disponibles et vous devez choisir celui qui convient.

Étape 4 Spécifiez le type de renseignements que l'option renvoie au client DHCP dans la zone **Option Data** (Données de l'option). Pour les options DHCP standard, seul le type de valeur d'option pris en charge est disponible. Pour toutes les autres options DHCP, tous les types de valeurs d'options sont disponibles. Cliquez sur **Add** (Ajouter) pour ajouter l'option à la liste des options DHCP. Cliquez sur **Delete** (Supprimer) pour supprimer l'option de la liste des options DHCP.

- Cliquez sur **IP Address** (Adresse IP) pour indiquer qu'une adresse IP est renvoyée au client DHCP. Vous pouvez spécifier jusqu'à deux adresses IP. L'adresse IP 1 et l'adresse IP 2 indiquent une adresse IP, en notation décimale à points.

Remarque Le nom des champs d'adresse IP associés peut changer en fonction de l'option DHCP que vous avez choisie. Par exemple, si vous choisissez l'option DHCP 3 (routeur), les noms des champs passent à Routeur 1 et Routeur 2.

- Cliquez sur **ASCII** pour indiquer qu'une valeur ASCII est renvoyée au client DHCP. Saisissez une chaîne de caractères ASCII dans le champ **Data** (Données). La chaîne de caractères ne peut pas inclure d'espaces.

Remarque Le nom du champ de données associé peut changer en fonction de l'option DHCP que vous avez choisie. Par exemple, si vous choisissez l'option DHCP 14 (fichier de vidage Merit), les noms des champs Data (Données) associés passent à File Name (Nom de fichier).

- Cliquez sur **Hex** pour spécifier qu'une valeur hexadécimale est renvoyée au client DHCP. Saisissez une chaîne hexadécimale avec un nombre pair de chiffres et sans espaces dans le champ **Data** (Données). Vous n'avez pas besoin d'utiliser le préfixe 0x.

Remarque Le nom du champ de données associé peut changer en fonction de l'option DHCP que vous avez choisie. Par exemple, si vous choisissez l'option DHCP 2 (décalage horaire), le champ Data (Données) associé devient le champ Offset (Décalage).

Étape 5 Cliquez sur **OK** pour fermer la boîte de dialogue **Advanced DHCP Options** (Options DHCP avancées).

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer le serveur sans état DHCPv6

Pour les clients qui utilisent SLAAC (StateLess Address Auto Configuration) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6, à la page 711), vous pouvez configurer l'ASA pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les

paquets IR et n'affecte pas d'adresses aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que l'ASA a reçu à l'aide de la délégation de préfixe.

Avant de commencer

Cette fonctionnalité n'est prise en charge qu'en mode routé simple. Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe.

Procédure

Étape 1 Configurez l'ensemble d'adresses DHCP IPv6 qui contient les informations que vous souhaitez que le serveur DHCPv6 fournisse :

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Pool (Bassin DHCP)**, puis cliquez sur **Add** (Ajouter).

b) Dans le champ **DHCP Pool Name** (Nom de l'ensemble DHCP), saisissez un nom.

c) Pour chaque paramètre de chaque onglet, cochez la case **Importer** ou saisissez manuellement une valeur dans le champ et cliquez sur **Add** (Ajouter).

L'option **Importer** utilise un ou plusieurs paramètres que l'ASA a obtenus du serveur DHCPv6 sur l'interface client de délégation de préfixe. Vous pouvez combiner des paramètres configurés manuellement avec des paramètres importés; cependant, vous ne pouvez pas configurer le même paramètre manuellement et spécifier également **Importer**.

d) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Étape 2 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 3 Choisissez une interface et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (modifier l'interface) s'affiche sous l'onglet **General** (général).

Étape 4 Cliquez sur l'onglet **IPv6**.

Étape 5 Dans la zone **Interface IPv6 DHCP**, cliquez sur le bouton radio **Server DHCP Pool Name** (nom de l'ensemble DHCP du serveur), puis saisissez le nom du regroupement DHCP IPv6.

Étape 6 **Enable DHCP for IPv6 non-address configuration** (activer DHCP pour la configuration sans adresse IPv6) : Pour définir l'indicateur de configuration d'adresse autre dans le paquet de publication de routeur IPv6.

Cet indicateur signale aux clients d'autoconfiguration IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des informations supplémentaires de DHCPv6, telles que l'adresse du serveur DNS.

Étape 7 Cliquez sur **OK**.

Vous retournez au volet **Configuration > Device Setup > Interface Settings > Interfaces** (Configuration > Configuration du périphérique > Paramètres d'interface > Interfaces).

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer les agents de relais DHCP.

Lorsqu'une requête DHCP entre dans une interface, les serveurs DHCP auxquels l'ASA relaye la requête dépendent de votre configuration. Vous pouvez configurer les types de serveurs suivants :

- Serveurs DHCP spécifiques à l'interface : lorsqu'une requête DHCP entre dans une interface particulière, l'ASA ne relaye la requête qu'aux serveurs spécifiques à l'interface.
- Serveurs DHCP globaux : lorsqu'une requête DHCP entre dans une interface qui n'a pas de serveurs spécifiques à l'interface configurés, l'ASA relaye la requête à tous les serveurs globaux. Si l'interface comporte des serveurs propres à une interface, les serveurs globaux ne sont pas utilisés.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Relay (Relais DHCP)**.

Étape 2 Cochez les cases correspondant aux services que vous souhaitez pour chaque interface dans la zone **DHCP Relay Agent** (Agent de relais DHC).

- **IPv4 > DHCP Relay Enabled (Relais DHCP activé)**.
- **IPv4 > Set Route** (IPv4 > Définir la route) : modifie l'adresse de la passerelle par défaut dans le message DHCP du serveur en lui donnant celle de l'interface ASA qui est la plus proche du client DHCP, qui a relayé la requête DHCP initiale. Cette action permet au client de configurer sa route par défaut pour qu'elle pointe vers l'ASA, même si le serveur DHCP spécifie un routeur différent. S'il n'y a pas d'option de routeur par défaut dans le paquet, l'ASA en ajoute une contenant l'adresse de l'interface.
- **IPv6 > DHCP Relay Enabled (Relais DHCP activé)**.
- **Trusted Interface** (Interface de confiance) : spécifie une interface client DHCP en laquelle vous souhaitez avoir confiance. Vous pouvez configurer des interfaces en tant qu'interfaces de confiance pour conserver l'option 82 de DHCP. L'option 82 DHCP est utilisée par les commutateurs et les routeurs en aval pour la surveillance DHCP et la protection source IP. Normalement, si l'agent de relais DHCP ASA reçoit un paquet DHCP avec l'option 82 déjà définie, mais que le champ giaddr (qui spécifie l'adresse de l'agent de relais DHCP définie par ce dernier avant de transmettre le paquet au serveur) est réglé sur 0, l'ASA supprimera ce paquet par défaut. Vous pouvez désormais conserver l'option 82 et transférer le paquet en identifiant une interface comme interface de confiance. Vous pouvez également faire confiance à toutes les interfaces en cochant la case **Set dhcp relay information as trusted on all interfaces** (Définir les renseignements de relais dhcp comme de confiance sur toutes les interfaces).

Étape 3 Ajoutez un ou plusieurs serveurs DHCP vers lesquels les requêtes DHCP sont relayées dans la zone **Global DHCP Relay Servers** (Serveurs relais DHCP globaux).

a) Cliquez sur **Add** (ajouter). La boîte de dialogue **Add Global DHCP Relay Server** (Ajouter un serveur relais DHCP global) apparaît.
b) Dans le champ **DHCP Server** (Serveur DHCP), saisissez l'adresse IPv4 ou IPv6 du serveur DHCP.
c) Choisissez l'interface à laquelle le serveur DHCP spécifié est connecté dans la liste déroulante **Interface**.
d) Cliquez sur **OK**.

Le serveur relais DHCP global nouvellement ajouté apparaît dans la liste **Global DHCP Relay Servers** (Serveurs relais DHCP globaux).

Étape 4 (Facultatif) Dans le champ **IPv4 Timeout** (Délai d'expiration IPv4), saisissez la durée, en secondes, autorisée pour le traitement des adresses DHCPv4. Les valeurs valides vont de 1 à 3 600 secondes. La valeur par défaut est 60 secondes.

Étape 5 (Facultatif) Dans le champ **IPv6 Timeout** (Délai d'expiration IPv6), saisissez la durée, en secondes, autorisée pour le traitement des adresses DHCPv6. Les valeurs valides vont de 1 à 3 600 secondes. La valeur par défaut est 60 secondes.

Étape 6 Dans la zone **DHCP Relay Interface Servers** (Serveurs d'interface de relais DHCP), ajoutez un ou plusieurs serveurs DHCP spécifiques à l'interface auxquels les requêtes DHCP sur une interface donnée sont relayées :

a) Cliquez sur **Add** (ajouter). La boîte de dialogue **Add DHCP Relay Server** (Ajouter un serveur relais DHCP) apparaît.

b) Dans la liste déroulante **Interface**, choisissez l'interface connectée aux clients DHCP. Notez que vous ne spécifiez pas l'interface de sortie pour les requêtes, comme pour un serveur DHCP global; au lieu de cela, l'ASA utilise la table de routage pour déterminer l'interface de sortie.

c) Dans le champ **Server to** (Serveur vers), saisissez l'adresse IPv4 du serveur DHCP, puis cliquez sur **Add** (Ajouter). Le serveur est ajouté à la liste de droite. Ajoutez jusqu'à 4 serveurs, si disponibles parmi le nombre maximum global. IPv6 n'est pas pris en charge pour les serveurs spécifiques à une interface.

d) Cliquez sur **OK**.

Les serveurs relais DHCP de l'interface nouvellement ajoutés apparaissent dans la liste **DHCP Relay Interface Servers** (Serveurs d'interface de relais DHCP).

Étape 7 Pour configurer toutes les interfaces en tant qu'interfaces de confiance, cochez la case **Set dhcp relay information as trusted on all interfaces** (Définir les renseignements de relais dhcp comme de confiance sur toutes les interfaces). Vous pouvez également faire confiance à des interfaces individuelles.

Étape 8 Cliquez sur **Apply** (appliquer) pour enregistrer vos paramètres.

Configuration du DNS dynamique

Lorsqu'une interface utilise l'adressage IP DHCP, l'adresse IP attribuée peut changer lors du renouvellement du bail DHCP. Lorsque l'interface doit être accessible à l'aide d'un nom de domaine complet (FQDN), le changement d'adresse IP peut rendre périmés les enregistrements de ressources du serveur DNS. Le DNS dynamique (DDNS) fournit un mécanisme pour mettre à jour les programmes de routage du DNS chaque fois que l'adresse IP ou le nom d'hôte change. Vous pouvez également utiliser DDNS pour les adresses IP statiques ou PPPoE.

DDNS met à jour les réflecteurs de routage suivants sur le serveur DNS : le RR A comprend le mappage nom-adresse IP, tandis que le RR PTR mappe les adresses aux noms.

L'ASA prend en charge les méthodes de mise à jour DDNS suivantes :

- DDNS standard : la méthode de mise à jour DDNS standard est définie par la RFC 2136.

  Avec cette méthode, l'ASA et le serveur DHCP utilisent les requêtes DNS pour mettre à jour les taux de renouvellement (RR) DNS. L'ASA ou le serveur DHCP envoie une requête DNS à son serveur DNS local pour obtenir des renseignements sur le nom d'hôte et, en fonction de la réponse, détermine le serveur

DNS principal qui possède les RR. L'ASA ou le serveur DHCP envoie ensuite une demande de mise à jour directement au serveur DNS principal. Consultez les scénarios typiques suivants.

- L'ASA met à jour le RR de A et le serveur DHCP met à jour le RR des PTR.

  En règle générale, l'ASA « possède » le RR de A, tandis que le serveur DHCP « possède » le taux de renouvellement (RR) PTR, de sorte que les deux entités doivent demander les mises à jour séparément. Lorsque l'adresse IP ou le nom d'hôte change, l'ASA envoie une requête DHCP (y compris l'option FQDN) au serveur DHCP pour l'informer qu'il doit demander une mise à jour des RR du PTR.

- Le serveur DHCP met à jour les taux de renouvellement A et PTR.

  Utilisez ce scénario si l'ASA n'a pas l'autorité pour mettre à jour le RR de A. Lorsque l'adresse IP ou le nom d'hôte change, l'ASA envoie une requête DHCP (y compris l'option FQDN) au serveur DHCP pour l'informer qu'il doit demander une mise à jour des RR A et PTR.

Vous pouvez configurer différentes propriétés en fonction de vos besoins en matière de sécurité et des exigences du serveur DNS principal. Par exemple, pour une adresse statique, l'ASA doit être propriétaire des mises à jour pour les deux enregistrements.

- Web : la méthode de mise à jour Web utilise la spécification de l'API distante DynDNS. (https://help.dyn.com/remote-access-api/).

  Avec cette méthode, lorsque l'adresse IP ou le nom d'hôte change, l'ASA envoie une requête HTTP directement à un fournisseur DNS auprès duquel vous avez un compte.

Remarque DDNS n'est pas pris en charge sur les interfaces BVI ou de membre du groupe de ponts.

Avant de commencer

- Configurez un serveur DNS sur **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**. Consultez Configurer des serveurs DNS, à la page 768.
- Configurez le nom d'hôte et le nom de domaine du périphérique dans **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)**. Consultez Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet, à la page 759. Si vous ne spécifiez pas de nom d'hôte par interface, le nom d'hôte du périphérique est utilisé. Si vous ne spécifiez pas de FQDN, pour l'adressage IP statique ou PPPoE, le nom de domaine du système ou le nom de domaine du serveur DNS est ajouté au nom d'hôte.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **Dynamic DNS (DNS dynamique)**.

Étape 2 Méthode standard DDNS : configurez une méthode de mise à jour DDNS pour activer les requêtes DNS de l'ASA.

Vous n'avez pas besoin de configurer une méthode de mise à jour DDNS si le serveur DHCP effectue toutes les demandes.

a) Dans la zone **Update Methods** (Méthodes de mise à jour), cliquez sur **Add** (Ajouter).
b) Spécifiez un **Name** (Nom) pour cette méthode.
c) (Facultatif) Configurez l'**intervalle de mise à jour** entre les requêtes DNS. Par défaut, lorsque toutes les valeurs sont définies sur 0, des demandes de mise à jour sont envoyées à chaque changement de l'adresse IP ou du nom d'hôte. Pour envoyer des demandes régulièrement, définissez les paramètres **Days** (0-364), **Hours**, **Minutes** et **Seconds** Jours, Heures, Minutes, secondes).
d) Choisissez **DDNS Record Type (Type d'enregistrement DDNS)** > **Standard DDNS (DDNS standard)**.
e) Sous **Records to Update** (Enregistrements à mettre à jour), spécifiez les enregistrements DDNS standard que vous souhaitez que l'ASA mette à jour.

   Ce paramètre affecte uniquement les enregistrements que vous souhaitez mettre à jour directement à partir de l'ASA; pour déterminer les enregistrements que vous souhaitez que le serveur DHCP mette à jour, configurez les paramètres du client DHCP par interface ou globalement. Voir l'étape Étape 4, à la page 795.

   - **Both (PTR and A records)** (Enregistrements PTR et A) : définit l'ASA pour qu'il mette à jour les enregistrements RR A et PTR. Utilisez cette option pour les adresses IP statiques ou PPPoE.
   - **A records only** (Enregistrements A uniquement) : définit l'ASA pour qu'il mette à jour les RR A uniquement. Utilisez cette option si vous souhaitez que le serveur DHCP mette à jour le RR des PTR.

f) Cliquez sur **OK**.
g) Attribuez cette méthode à l'interface dans l'étape Étape 4, à la page 795.

Étape 3 Méthode Web : configurez une méthode de mise à jour DDNS pour activer les demandes de mise à jour HTTP à partir de l'ASA.

a) Dans la zone **Update Methods** (Méthodes de mise à jour), cliquez sur **Add** (Ajouter).
b) Spécifiez un **Name** (Nom) pour cette méthode.
c) (Facultatif) Configurez l'**intervalle de mise à jour** entre les requêtes DNS. Par défaut, lorsque toutes les valeurs sont définies sur 0, des demandes de mise à jour sont envoyées à chaque changement de l'adresse IP ou du nom d'hôte. Pour envoyer des demandes régulièrement, définissez les paramètres **Days** (0-364), **Hours**, **Minutes** et **Seconds** Jours, Heures, Minutes, secondes).
d) Choisissez **DDNS Record Type (Type d'enregistrement DDNS)** > **Web**.
e) Dans le champ **Web**, spécifiez l'URL de mise à jour. Vérifiez auprès de votre fournisseur DNS pour connaître l'URL requise.

   Utilisez la syntaxe suivante :

   https://*username (nom d'utilisateur)***:***password (mot de passe)***@***provider-domain (domaine du fournisseur)*/*path (chemin)***?hostname=<h>&myip=<a>**

   Exemple :

   https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>

f) Pour **Web Update Type** (Type de mise à jour Web), spécifiez les types d'adresses (IPv4 ou IPv6) que vous souhaitez mettre à jour.

   - **Both All** (Toutes) : (par défaut) met à jour toutes les adresses IPv4 et IPv6.
   - **Both** (Les deux) : met à jour l'adresse IPv4 et la dernière adresse IPv6.
   - **IPv4** : met à jour uniquement l'adresse IPv4.

- **IPv6** : met à jour uniquement la dernière adresse IPv6.
- **IPv6 All** (Toutes les IPv6) : met à jour toutes les adresses IPv6.

g) Dans **Reference Identity Name** (Nom d'identité de référence), saisissez le nom d'identité de référence configuré pour valider l'identité du certificat du serveur.

h) Cliquez sur **OK**.

i) Attribuez cette méthode à l'interface dans l'étape Étape 4, à la page 795.

j) La méthode de type Web pour DDNS nécessite également que vous identifiiez l'autorité de certification racine du serveur DDNS pour valider le certificat du serveur DDNS pour la connexion HTTPS. Voir l'étape Étape 6, à la page 796.

Étape 4 Configurez les paramètres d'interface pour DDNS, y compris la définition de la méthode de mise à jour, les paramètres du client DHCP et le nom d'hôte pour cette interface.

a) Dans la zone **Dynamic DNS Interface Settings** (Paramètres d'interface DNS dynamique), cliquez sur **Add** (Ajouter).

b) Choisissez **l'interface** dans la liste déroulante.

c) Choisissez le **Method Name** (Nom de la méthode) que vous avez créé dans la zone **Update Methods** (Méthodes de mise à jour).

(Méthode DDNS standard) Vous n'avez pas besoin d'attribuer de méthode si vous souhaitez que le serveur DHCP effectue toutes les mises à jour.

d) Définissez le **Hostname** (Nom d'hôte) pour cette interface.

Si vous ne définissez pas de nom d'hôte, le nom d'hôte du périphérique est utilisé. Si vous ne spécifiez pas de FQDN, le nom de domaine système ou le domaine par défaut du groupe de serveurs DNS est ajouté (pour les adresses IP statiques ou PPPoE) ou le nom de domaine du serveur DHCP est ajouté (pour les adresses IP DHCP).

e) Méthode DDNS standard : configurez le champ **DHCP Server Record Updates** (Mises à jour des enregistrements du serveur DHCP) afin de déterminer quels enregistrements vous souhaitez que le serveur DHCP mette à jour.

L'ASA envoie les requêtes des clients DHCP au serveur DHCP. Notez que le serveur DHCP doit également être configuré pour prendre en charge DDNS. Le serveur peut être configuré pour répondre aux demandes du client ou il peut remplacer les commandes du client (auquel cas, il répondra au client pour que le client n'essaye pas également d'effectuer les mises à jour effectuées par le serveur). Même si le client ne demande pas de mises à jour DDNS, le serveur DHCP peut être configuré pour envoyer quand même des mises à jour.

Pour les adresses IP statiques ou PPPoE, ces paramètres sont ignorés.

Remarque Vous pouvez également définir ces valeurs globalement pour toutes les interfaces sur la page principale **Dynamic DNS** (DNS dynamique). Les paramètres par interface prévalent sur les paramètres globaux.

- **Default (PTR Records)** (Par défaut (Enregistrements PTR)) : demande au serveur DHCP d'effectuer la mise à jour des RR PTR. Ce paramètre fonctionne conjointement avec une méthode de mise à jour DDNS avec les **enregistrements A** activés.

- **Both (PTR Records and A Records)** (Les deux (Enregistrements PTR et A)) : demande au serveur DHCP d'effectuer les mises à jour des enregistrements A et RR PTR. Ce paramètre ne nécessite pas l'association d'une méthode de mise à jour DDNS à l'interface.
- **None** (Aucune) : demande au serveur DHCP de ne pas effectuer de mises à jour. Ce paramètre fonctionne conjointement avec une méthode de mise à jour DDNS avec les **enregistrements A et PTR** activés.

f) Cliquez sur **OK**.

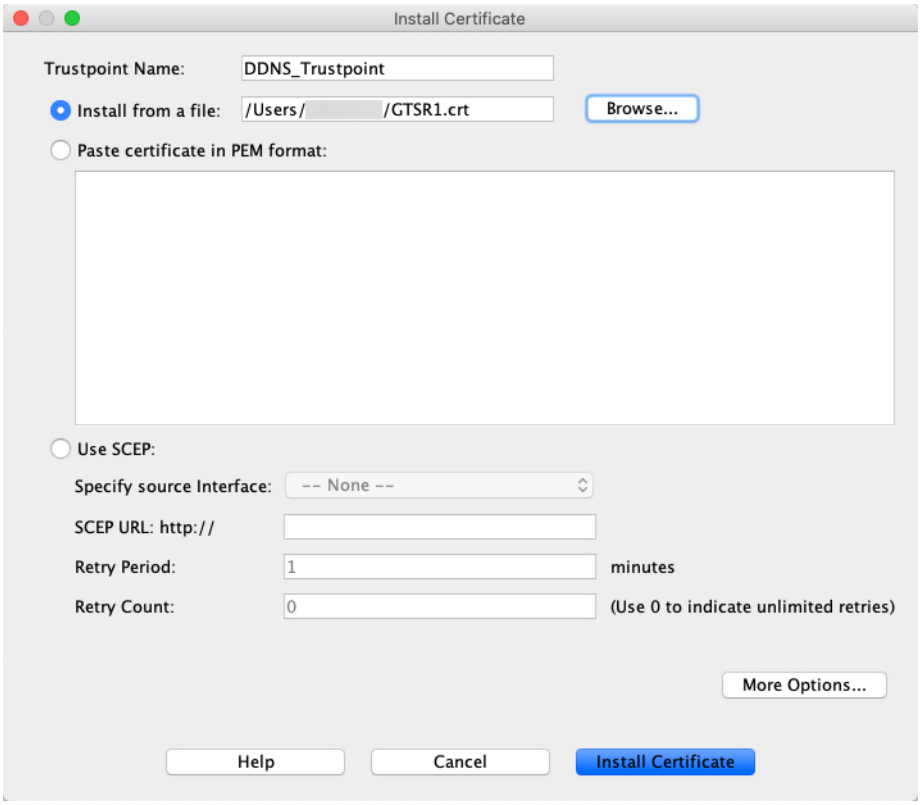
Étape 5 Cliquez sur **Apply** (Appliquer) pour enregistrer vos modifications ou sur **Reset** (Réinitialiser) pour les annuler et en saisir de nouvelles.

Étape 6 La méthode Web pour DDNS nécessite également que vous identifiiez l'autorité de certification racine du serveur DDNS pour valider le certificat du serveur DDNS pour la connexion HTTPS.

L'exemple suivant montre comment ajouter l'autorité de certification d'un serveur DDNS en tant que point de confiance.

a) Obtenez le certificat de l'autorité de certification du serveur DDNS. Cette procédure montre une importation de fichier, mais vous pouvez également le coller au format PEM.

b) Sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)**, puis cliquez sur **Add** (Ajouter).



c) Saisissez un **Trustpoint Name** (Nom de point de confiance).

d) Cliquez sur **Install from a file** (Installer à partir d'un fichier) et accédez au fichier de certificat.

e) Cliquez sur **Install Certificate** (Installer le certificat).

Supervision des services DHCP et DDNS

Cette section comprend les procédures pour superviser les services DHCP et DDNS.

Supervision des services DHCP

- **Monitoring (Supervision) > Interfaces > DHCP > DHCP Client Lease Information (Renseignements sur le bail locatif du client DHCP)**.

  Ce volet affiche les adresses IP configurées des clients DHCP.

- **Monitoring (Supervision) > Interfaces > DHCP > DHCP Server Table (Tableau des serveurs DHCP)**

  Ce volet affiche les adresses IP dynamiques configurées des clients DHCP.

- **Monitoring (Supervision) > Interfaces > DHCP > DHCP Statistics (Statistiques DHCP)**

  Ce volet affiche les types de messages DHCPv4, les compteurs, les valeurs, les directions, les messages reçus et les messages envoyés.

- **Monitoring (Supervision) > Interfaces > DHCP > IPV6 DHCP Relay Statistics (Statistiques de relais DHCP IPV6)**

  Ce volet affiche les types de messages de relais DHCPv6, les compteurs, les valeurs, les directions, les messages reçus et les messages envoyés.

- **Monitoring (Supervision) > Interfaces > DHCP > IPV6 DHCP Relay Binding (Liaison de relais DHCP IPV6)**

  Ce volet affiche les liaisons de relais DHCPv6.

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **IPV6 DHCP Interface Statistics (Statistiques d'interface DHCP IPV6)**

  Cet écran affiche les renseignements DHCPv6 pour toutes les interfaces. Si l'interface est configurée pour la configuration du serveur sans état DHCPv6 (voir Configurer le serveur sans état DHCPv6, à la page 789), cet écran répertorie l'ensemble DHCPv6 utilisé par le serveur. Si l'interface a une configuration de client d'adresse DHCPv6 ou de client de délégation de préfixe, cet écran affiche l'état de chaque client et les valeurs reçues du serveur. Cet écran affiche également les statistiques des messages pour le serveur ou le client DHCP.

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **IPV6 DHCP HA Statistics (Statistiques DHCP IPV6 à haute disponibilité)**

  Cet écran affiche les statistiques de transaction entre les unités de basculement, y compris le nombre de fois où les renseignements DUID ont été synchronisés entre les unités.

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **IPV6 DHCP Server Statistics (Statistiques de serveur DHCP IPV6)**

  Cet écran affiche les statistiques du serveur sans état DHCPv6.

Supervision de l'état DDNS

Consultez la commande suivante pour superviser l'état du DDNS. Saisissez les commandes dans **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**.

- **show ddns update** {**interface** *if_name* | **method** [*name*]}

  Cette commande affiche l'état de la mise à jour du DDNS.

  L'exemple suivant montre les détails de la méthode de mise à jour du DDNS :

```
ciscoasa# show ddns update method ddns1

Dynamic DNS Update Method: ddns1
  IETF standardized Dynamic DNS 'A' record update
```

  L'exemple suivant montre les détails de la méthode de mise à jour Web :

```
ciscoasa# show ddns update method web1

Dynamic DNS Update Method: web1
 Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
https://cdarwin:*****@ddns.cisco.com/update?hostname=<h>&myip=<a>
```

  L'exemple suivant montre les renseignements relatifs à l'interface DDNS :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available
```

  L'exemple suivant montre une mise à jour de type Web réussie :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : asa1.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

  L'exemple suivant montre une défaillance de type Web :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

  L'exemple suivant montre que le serveur DNS a renvoyé une erreur pour la mise à jour du type Web :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

L'exemple suivant montre qu'une mise à jour Web n'a pas encore été tentée en raison de l'adresse IP non configurée ou de l'échec de la requête DHCP, par exemple :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update Not attempted
```

Historique des services DHCP et DDNS

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de DDNS pour la méthode de mise à jour Web	9.15(1)	Vous pouvez maintenant configurer une interface pour utiliser DDNS avec la méthode de mise à jour Web. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **Dynamic DNS (DNS dynamique)**
Prise en charge du serveur de relais DHCP sur les VTI	9.14(1)	Vous pouvez maintenant activer le relais DHCP sur les VTI. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Relay (Relais DHCP)** > **DHCP Relay Interface Servers (Serveurs d'interface de relais DHCP)**
Réservation DHCP	9.13(1)	L'ASA prend en charge la réservation DHCP. Le serveur DHCP attribue une adresse IP statique à partir de l'ensemble d'adresses à un client DHCP en fonction de l'adresse MAC du client. Commandes nouvelles ou modifiées : **dhcpd reserve-address** . ASDM n'est pas pris en charge.

Nom de la caractéristique	Versions de plateforme	Description
DHCP IPv6	9.6(2)	L'ASA prend désormais en charge les fonctionnalités suivantes pour l'adressage IPv6 : • Client d'adresse DHCPv6 : l'ASA obtient une adresse globale IPv6 et une route par défaut facultative du serveur DHCPv6. • Client de délégation de préfixe DHCPv6 : l'ASA obtient le ou les préfixes délégués d'un serveur DHCPv6. L'ASA peut ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface ASA afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. • Annonce de routeur BGP pour les préfixes délégués • Serveur sans état DHCPv6 : l'ASA fournit d'autres renseignements tels que le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresses aux clients. Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add Interface (Ajouter une interface)** > **IPv6** **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Pool (Réserve DHCP)** **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv6 Family (Famille IPv6)** > **Networks (Réseaux)** **Monitoring (Supervision)** > **Interfaces** > **DHCP**
Supervision DHCPv6	9.4(1)	Vous pouvez maintenant superviser les statistiques DHCP pour IPv6 et les liaisons DHCP pour IPv6. Nous avons introduit les écrans suivants : Supervision DHCPv6 Monitoring (Supervision) > Interfaces > DHCP > IPV6 DHCP Statistics (Statistiques DHCP IPV6), Monitoring (Supervision) > Interfaces > DHCP > IPV6 DHCP Binding (Liaison DHCP IPV6).
Le serveur de relais DHCP valide l'identifiant du serveur DHCP pour les réponses	9.2(4)/9.3(3)	Si le serveur de relais DHCP ASA reçoit une réponse d'un serveur DHCP incorrect, il vérifie désormais que la réponse provient du bon serveur avant de donner suite à la réponse. Nous n'avons pas introduit ni modifié de commandes. Nous n'avons pas modifié d'écrans ASDM. Nous n'avons pas modifié d'écrans ASDM.
Fonction de liaison DHCP	9.1(4)	Pendant la phase de liaison DHCP, le client tente maintenant de se rétablir d'autres serveurs DHCP dans la liste des groupes du tunnel. Avant cette version, le client ne se reconnectait pas à un autre serveur lorsque le renouvellement du bail DHCP échouait. Nous n'avons pas modifié d'écrans ASDM.

Nom de la caractéristique	Versions de plateforme	Description
Interfaces de confiance DHCP	9.1(2)	Vous pouvez désormais configurer des interfaces en tant qu'interfaces de confiance pour conserver l'option 82 de DHCP. L'option 82 DHCP est utilisée par les commutateurs et les routeurs en aval pour la surveillance DHCP et la protection source IP. Normalement, si l'agent de relais DHCP ASA reçoit un paquet DHCP avec l'option 82 déjà définie, mais que le champ giaddr (qui spécifie l'adresse de l'agent de relais DHCP définie par ce dernier avant de transmettre le paquet au serveur) est réglé sur 0, l'ASA supprimera ce paquet par défaut. Vous pouvez désormais conserver l'option 82 et transférer le paquet en identifiant une interface comme interface de confiance. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > DHCP > DHCP Relay (Relais DHCP).
Serveurs de relais DHCP par interface (IPv4 uniquement)	9.1(2)	Vous pouvez désormais configurer des serveurs de relais DHCP par interface, de sorte que les demandes qui entrent dans une interface donnée ne sont relayées que vers les serveurs spécifiés pour cette interface. IPv6 n'est pas pris en charge pour le relais DHCP par interface. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > DHCP > DHCP Relay (Relais DHCP).
Relais DHCP pour IPv6 (DHCPv6)	9.0(1)	La prise en charge des relais DHCP pour IPv6 a été ajoutée. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > DHCP > DHCP Relay (Relais DHCP).
Système de nom de domaine dynamique (DDNS)	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > DNS > DNS Client (Client DNS). Configuration > Device Management (Gestion des périphériques) > DNS > Dynamic DNS (DNS dynamique).
DHCP (protocole de configuration dynamique des hôtes)	7.0(1)	L'ASA peut fournir un serveur DHCP ou des services de relais DHCP aux clients DHCP connectés aux interfaces ASA. Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > DHCP > DHCP Relay (Relais DHCP). Configuration > Device Management (Gestion des périphériques) > DHCP > DHCP Server (Serveur DHCP).



CHAPITRE 26

Certificats numériques

Ce chapitre décrit comment configurer les certificats numériques.

- À propos des certificats numériques, à la page 803
- Lignes directrices pour les certificats numériques, à la page 811
- Configurer les certificats numériques, à la page 814
- Définir une alerte d'expiration de certificat (pour les certificats d'identité ou CA), à la page 831
- Supervision des certificats numériques, à la page 832
- Historique de gestion des certificats, à la page 832

À propos des certificats numériques

Les certificats numériques fournissent une identification numérique aux fins d'authentification. Un certificat numérique contient des renseignements permettant d'identifier un appareil ou un utilisateur, tels que le nom, le numéro de série, l'entreprise, le service ou l'adresse IP. Les autorités de certification sont chargées de gérer les demandes de certificat et d'émettre des certificats numériques. Les autorités de certification sont des autorités de confiance qui « signent » des certificats pour vérifier leur authenticité, garantissant ainsi l'identité du périphérique ou de l'utilisateur.

Un certificat numérique inclut également une copie de la clé publique de l'utilisateur ou du périphérique. Une autorité de certification peut être un tiers de confiance, comme VeriSign, ou une autorité de certification privée (interne) que vous établissez au sein de votre organisation. Les autorités de certification émettent des certificats numériques dans le contexte d'une PKI, qui utilise le chiffrement par clé publique ou par clé privée pour assurer la sécurité.

Pour l'authentification à l'aide de certificats numériques, au moins un certificat d'identité et son certificat CA d'émission doivent exister sur un ASA. Cette configuration autorise plusieurs identités, racines et hiérarchies de certificat. L'ASA évalue les certificats tiers par rapport aux CRL, également appelées listes de révocation d'autorité, depuis le certificat d'identité jusqu'à la chaîne des autorités de certification subordonnées.

Voici une description de plusieurs types de certificats numériques disponibles :

- Un certificat d'autorité de certification est utilisé pour signer les autres certificats. Il est autosigné et appelé certificat racine. Un certificat émis par un autre certificat CA s'appelle un certificat subordonné.
- Les autorités de certification délivrent également des certificats d'identité, qui sont des certificats pour des systèmes ou des hôtes spécifiques.
- Les certificats de signataire de code sont des certificats spéciaux utilisés pour créer des signatures numériques pour signer le code, le code signé révélant lui-même l'origine du certificat.

Dans une hiérarchie avec une racine et deux certificats CA intermédiaires, une validation de CRL pour l'accès à distance échoue sur la tête de réseau exécutant la version 9.13 ou une version ultérieure lorsque le certificat d'ID est signé par une CA intermédiaire, mais que la CRL est signée par une autre CA intermédiaire. La défaillance se produit même si la tête de réseau fait confiance aux deux intermédiaires lorsque ceux-ci sont signés par la même racine.

Par conséquent, chaque signataire doit conserver sa propre CRL. Chaque signataire précisera ensuite l'emplacement de la CRL dans la liste d'URL de chaque certificat qu'il signe. Sinon, vous pouvez configurer un remplacement d'URL dans le point de confiance de chaque signataire pointant vers le bon emplacement de CRL.

La CA locale intègre une fonctionnalité d'autorité de certificat indépendante sur l'ASA, déploie les certificats et assure une vérification sécurisée de la révocation des certificats émis. La CA locale fournit une autorité interne sécurisée et configurable pour l'authentification des certificats avec inscription des utilisateurs via une page de connexion au site Web.

Remarque Les certificats CA et les certificats d'identité s'appliquent à la fois aux connexions VPN de site à site et aux connexions VPN d'accès à distance. Les procédures dans ce document font référence à l'utilisation du VPN d'accès à distance dans l'interface graphique utilisateur du gestionnaire ASDM.

Astuces Pour un exemple de scénario comprenant la configuration des certificats et l'équilibrage de charges, consultez l'URL suivante : https://supportforums.cisco.com/docs/DOC-5964.

Cryptographie à clé publique

Les signatures numériques, activées par le chiffrement à clé publique, fournissent un moyen d'authentifier les appareils et les utilisateurs. Dans le chiffrement à clé publique, comme le système de chiffrement RSA, chaque utilisateur dispose d'une paire de clés contenant une clé publique et une clé privée. Les clés agissent comme des compléments, et tout ce qui est chiffré avec l'une des clés peut être déchiffré avec l'autre.

En termes simples, une signature se forme lorsque les données sont chiffrées avec une clé privée. La signature est jointe aux données et envoyée au récepteur. Le récepteur applique la clé publique de l'expéditeur aux données. Si la signature envoyée avec les données correspond au résultat de l'application de la clé publique aux données, la validité du message est établie.

Ce processus repose sur le récepteur ayant une copie de la clé publique de l'expéditeur et sur un degré élevé de confiance que cette clé appartient à l'expéditeur, et non à une personne se faisant passer pour l'expéditeur.

L'obtention de la clé publique d'un expéditeur est normalement gérée en externe ou par le biais d'une opération effectuée lors de l'installation. Par exemple, la plupart des navigateurs Web sont configurés avec les certificats racine de plusieurs autorités de certification par défaut. Pour le VPN, le protocole IKE, un composant IPsec, peut utiliser des signatures numériques pour authentifier les périphériques homologues avant de configurer des associations de sécurité.

Évolutivité des certificats

Sans certificats numériques, vous devez configurer manuellement chaque homologue IPsec pour chaque homologue avec lequel il communique; par conséquent, chaque nouvel homologue que vous ajoutez à un réseau nécessite une modification de configuration sur chaque homologue avec lequel il doit communiquer de manière sécurisée.

Lorsque vous utilisez des certificats numériques, chaque homologue est inscrit auprès d'une CA. Lorsque deux homologues tentent de communiquer, ils échangent des certificats et signent numériquement les données pour s'authentifier. Lorsqu'un nouvel homologue est ajouté au réseau, vous inscrivez cet homologue auprès d'une CA et aucun des autres homologues ne nécessite de modification. Lorsque le nouvel homologue tente une connexion IPsec, les certificats sont automatiquement échangés et l'homologue peut être authentifié.

Avec une CA, un homologue s'authentifie auprès de l'homologue distant en lui envoyant un certificat et en effectuant une cryptographie à clé publique. Chaque homologue envoie son certificat unique, qui a été émis par la CA. Ce processus fonctionne, car chaque certificat encapsule la clé publique de l'homologue associé, chaque certificat est authentifié par la CA et tous les homologues participants reconnaissent la CA comme une autorité d'authentification. Le processus s'appelle IKE avec une signature RSA.

L'homologue peut continuer à envoyer son certificat pour plusieurs sessions IPsec et à plusieurs homologues IPsec jusqu'à l'expiration du certificat. Lorsque son certificat expire, l'administrateur homologue doit en obtenir un nouveau auprès de la CA.

Les CA peuvent également révoquer les certificats d'homologues qui ne participent plus à IPsec. Les certificats révoqués ne sont pas reconnus comme valides par les autres homologues. Les certificats révoqués sont répertoriés dans une CRL, que chaque homologue peut vérifier avant d'accepter un certificat d'un autre homologue.

Certaines CA disposent d'une autorité d'enregistrement dans le cadre de leur mise en œuvre. Une autorité d'enregistrement est un serveur qui agit en tant que mandataire pour la CA, de sorte que les fonctions CA puissent continuer à fonctionner lorsque la CA n'est pas disponible.

Paires de clés

Les paires de clés sont des clés d'algorithme de signature numérique à courbe elliptique (ECDSA), qui ont les caractéristiques suivantes :

- Les clés RSA peuvent être utilisées pour SSH ou SSL.
- L'inscription SCEP prend en charge la certification des clés RSA.
- La taille de clé RSA maximum est de 4 096 et la valeur par défaut est de 2 048.
- La longueur maximum de la clé ECDSA est de 521, et la valeur par défaut est de 384.
- Vous pouvez générer une paire de clés RSA à usage général, utilisée à la fois pour la signature et le chiffrement, ou vous pouvez générer des paires de clés RSA distinctes pour chaque objectif. Des clés de signature et de chiffrement distinctes aident à réduire l'exposition des clés, car SSL utilise une clé pour le chiffrement, mais pas pour la signature. Cependant, IKE utilise une clé pour la signature, mais pas pour le chiffrement. En utilisant des clés distinctes pour chacune, l'exposition des clés est réduite au minimum.

Point de confiance

Les points de confiance vous permettent de gérer et de suivre les autorités de certification et les certificats. Un point de confiance est la représentation d'une autorité de certification ou d'une paire d'identités. Un point de confiance comprend l'identité de l'autorité de certification, des paramètres de configuration spécifiques à l'autorité de certification et une association avec un certificat d'identité inscrit.

Après avoir défini un point de confiance, vous pouvez le référencer par son nom dans les commandes nécessitant de spécifier une CA. Vous pouvez configurer de nombreux points de confiance.



Remarque Si l'ASA a plusieurs points de confiance qui partagent la même CA, un seul de ces points de confiance partageant la CA peut être utilisé pour valider les certificats d'utilisateur. Pour contrôler le partage du point de confiance qu'une CA utilise pour la validation des certificats d'utilisateur émis par cette CA, utilisez la commande **support-user-cert-validation**.

Pour l'inscription automatique, un point de confiance doit être configuré avec une URL d'inscription, et la CA que représente le point de confiance doit être disponible sur le réseau et doit prendre en charge SCEP.

Vous pouvez exporter et importer la paire de clés et les certificats émis associés à un point de confiance au format PKCS12. Ce format est utile pour dupliquer manuellement une configuration de point de confiance sur un autre ASA.

Inscription de certificat

L'ASA a besoin d'un certificat CA pour chaque point de confiance et d'un ou deux certificats pour lui-même, selon la configuration des clés utilisées par le point de confiance. Si le point de confiance utilise des clés RSA distinctes pour la signature et le chiffrement, l'ASA a besoin de deux certificats, un pour chaque fonction. Dans les autres configurations de clés, un seul certificat est nécessaire.

L'ASA prend en charge l'inscription automatique avec SCEP et l'inscription manuelle, ce qui vous permet de coller un certificat codé en base 64 directement dans le terminal. Pour les VPN de site à site, vous devez inscrire chaque ASA. Pour les VPN d'accès à distance, vous devez inscrire chaque ASA et chaque client VPN d'accès à distance.

Serveur mandataire pour les demandes SCEP

L'ASA peut servir de mandataire pour les demandes SCEP entre Secure Client (services client sécurisés) et une CA tierce. La CA ne doit être accessible à l'ASA que si celui-ci agit en tant que mandataire. Pour que l'ASA fournisse ce service, l'utilisateur doit s'authentifier à l'aide de l'une des méthodes prises en charge par AAA avant que l'ASA envoie une demande d'inscription. Vous pouvez également utiliser l'analyse de l'hôte et des politiques d'accès dynamique pour appliquer des règles d'admissibilité à l'inscription.

L'ASA prend en charge cette fonctionnalité uniquement avec une session VPN Secure Client (services client sécurisés) SSL ou IKEv2. Il prend en charge toutes les autorités de certification conformes à SCEP, y compris Cisco IOS CS, Windows Server 2003 CA et Windows Server 2008 CA

L'accès sans client (par navigateur) ne prend pas en charge le mandataire SCEP, bien que WebLaunch (Secure Client (services client sécurisés) initié sans client) le prenne en charge.

L'ASA ne prend pas en charge l'interrogation des certificats.

L'ASA prend en charge l'équilibrage de charges pour cette fonctionnalité.

Vérification de la révocation

Lorsqu'un certificat est émis, il est valide pour une période fixe. Parfois, une CA révoque un certificat avant l'expiration de cette période; par exemple, en raison de problèmes de sécurité ou d'un changement de nom ou d'association. Les CA publient périodiquement une liste signée des certificats révoqués. L'activation de la vérification de la révocation force l'ASA à vérifier que la CA n'a pas révoqué un certificat chaque fois qu'il l'utilise pour l'authentification.

Lorsque vous activez la vérification de la révocation, l'ASA vérifie l'état de révocation du certificat pendant le processus de validation du certificat PKI, qui peut utiliser la vérification des CRL, OCSP ou les deux. Le protocole OCSP est uniquement utilisé lorsque la première méthode renvoie une erreur (par exemple, indiquant que le serveur n'est pas disponible).

Lors de la vérification des CRL, l'ASA récupère, analyse et met en mémoire cache les CRL, qui fournissent une liste complète des certificats révoqués (et non révoqués) avec leurs numéros de série. L'ASA évalue les certificats en fonction des CRL, également appelées listes de révocation d'autorité, à partir du certificat d'identité jusqu'à la chaîne des autorités de certification subordonnées.

Le protocole OCSP offre une méthode plus évolutive de vérification de l'état de révocation dans la mesure où il localise l'état du certificat auprès d'une autorité de validation, à laquelle il demande l'état d'un certificat spécifique.

Serveurs CA pris en charge

L'ASA prend en charge les serveurs CA suivants :

CS Cisco IOS, CA local ASA et les prestataires CA tiers conformes à X.509, y compris, sans s'y limiter :

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

Les CRL fournissent à l'ASA un moyen de déterminer si un certificat qui se trouve dans sa plage de temps valide a été révoqué par la CA émettrice. La configuration des CRL fait partie de la configuration d'un point de confiance.

Vous pouvez configurer l'ASA pour rendre les vérifications de CRL obligatoires lors de l'authentification d'un certificat à l'aide de la commande **revocation-check crl**. Vous pouvez également rendre la vérification

de la CRL facultative en utilisant la commande **revocation-check crl none**, qui permet de réussir l'authentification par certificat lorsque la CA n'est pas disponible pour fournir des données CRL mises à jour.

Remarque La commande **revocation-check crl none**, qui a été supprimée dans la version 9.13(1), a été restaurée.

L'ASA peut récupérer les CRL des autorités de certification à l'aide de HTTP, SCEP ou LDAP. Les CRL extraites pour chaque point de confiance sont mises en cache pour une durée configurable pour chaque point de confiance.

Remarque Même si le serveur CRL répond par l'indicateur HTTP « Connection: Keep-alive » (Connexion : Keepalive) pour indiquer une connexion persistante, l'ASA ne demande pas la prise en charge de la connexion persistante. Modifiez les paramètres sur le serveur CRL pour répondre par « Connection: Close » (Connexion : Fermer) lorsque la liste est envoyée.

Lorsque l'ASA a mis en cache une CRL plus longtemps que la configuration de la mise en cache des CRL, l'ASA considère la CRL comme trop ancienne pour être fiable ou « obsolète ». L'ASA tente de récupérer une version plus récente de la CRL la prochaine fois qu'une authentification par certificat nécessite une vérification de la CRL obsolète.

Vous pourriez recevoir un échec de *vérification de la révocation* pour une connexion ou un certificat utilisateur si vous dépassez la limite de taille de 16 Mo pour la CRL.

L'ASA met les CRL en cache pendant une durée déterminée par les deux facteurs suivants :

- Le nombre de minutes spécifié avec la commande **cache-time**. La valeur par défaut est de 60 minutes.
- Le champ NextUpdate dans les CRL extraites, qui peut être absent des CRL. Vous contrôlez si l'ASA requiert et utilise le champ NextUpdate avec la commande **enforcenextupdate**.

L'ASA utilise ces deux facteurs de la manière suivante :

- Si le champ NextUpdate n'est pas obligatoire, l'ASA marque les CRL comme obsolètes après la durée définie par la commande **cache-time**.
- Si le champ NextUpdate est obligatoire, l'ASA marque les CRL comme obsolètes à la première des deux fois spécifiées par la commande **cache-time** et le champ NextUpdate. Par exemple, si la commande **cache-time** est définie à 100 minutes et que le champ NextUpdate indique que la prochaine mise à jour est à 70 minutes, l'ASA marque les CRL comme obsolètes en 70 minutes.

Si l'ASA a une mémoire insuffisante pour stocker toutes les CRL mises en cache pour un point de confiance donné, il supprime la CRL la moins récemment utilisée pour faire de la place pour une CRL nouvellement récupérée. Les grandes CRL nécessitent un surdébit de calcul important pour les analyser. Par conséquent, pour de meilleures performances, utilisez de nombreuses CRL de plus petite taille plutôt que quelques grandes CRL, ou de préférence, utilisez OCSP.

Consultez les tailles de cache suivantes :

- Mode de contexte unique : 128 Mo
- Mode de contexte multiple : 16 Mo par contexte

OCSP

L'OCSP fournit à l'ASA un moyen de déterminer si un certificat qui se trouve dans sa plage de temps valide a été révoqué par la CA émettrice. La configuration de l'OCSP fait partie de la configuration du point de confiance.

L'OCSP localise l'état du certificat sur une autorité de validation (un serveur OCSP, également appelé *répondeur*) que l'ASA interroge pour connaître l'état d'un certificat en particulier. Cette méthode offre une meilleure évolutivité et un état de révocation plus à jour que la vérification des CRL, et aide les entreprises avec de grandes installations PKI à déployer et à étendre des réseaux sécurisés.



Remarque L'ASA autorise un décalage de cinq secondes pour les réponses OCSP.

Vous pouvez configurer l'ASA pour rendre les vérifications OCSP obligatoires lors de l'authentification d'un certificat à l'aide de la commande **revocation-check ocsp**. Vous pouvez également rendre la vérification OCSP facultative en utilisant la commande **revocation-check ocsp none**, qui permet de réussir l'authentification par certificat lorsque l'autorité de validation n'est pas disponible pour fournir des données OCSP mises à jour.



Remarque La commande **revocation-check ocsp none**, qui a été supprimée dans la version 9.13(1), a été restaurée.

L'OCSP fournit trois façons de définir l'URL du serveur OCSP. L'ASA utilise ces serveurs dans l'ordre suivant :

1. L'URL OCSP définie dans une règle de remplacement de certificat de correspondance à l'aide de la commande **match certificate**).
2. L'URL OCSP configurée à l'aide de la commande **ocsp url**.
3. Le champ AIA du certificat client.



Remarque Pour configurer un point de confiance pour valider un certificat de répondeur OCSP autosigné, vous devez importer le certificat de répondeur autosigné dans son propre point de confiance en tant que certificat CA de confiance. Ensuite, vous devez configurer la commande **match certificate** dans le point de confiance de validation du certificat client pour utiliser le point de confiance qui comprend le certificat de répondeur OCSP autosigné pour valider le certificat de répondeur. Utilisez la même procédure pour configurer la validation des certificats de répondeur externes au chemin de validation du certificat client.

Le certificat du serveur OCSP (répondeur) signe généralement la réponse OCSP. Après avoir reçu la réponse, l'ASA tente de vérifier le certificat du répondeur. La CA définit normalement la durée de vie du certificat de répondeur OCSP sur une période relativement courte pour réduire au minimum les risques de compromission. La CA comprend généralement une extension ocsp-no-check dans le certificat du répondeur, qui indique que ce certificat n'a pas besoin de vérification de l'état de révocation. Cependant, si cette extension est absente, l'ASA tente de vérifier l'état de révocation en utilisant la même méthode que spécifiée dans le point de confiance. Si le certificat du répondeur n'est pas vérifiable, les vérifications de révocation échouent. Pour éviter cette possibilité, utilisez la commande **revocation-check none** pour configurer le point de confiance de validation du certificat du répondeur et utilisez la commande **revocation-check ocsp** pour configurer le certificat client.

Certificats et coordonnées de connexion de l'utilisateur

La section suivante décrit les différentes méthodes d'utilisation des certificats et des coordonnées de connexion de l'utilisateur (nom d'utilisateur et mot de passe) pour l'authentification et l'autorisation. Ces méthodes s'appliquent à IPsec, Secure Client (services client sécurisés) et au SSL VPN sans client.

Dans tous les cas, l'autorisation LDAP n'utilise pas le mot de passe comme identifiant. L'autorisation RADIUS utilise un mot de passe commun pour tous les utilisateurs ou le nom d'utilisateur comme mot de passe.

Informations d'authentification de l'utilisateur

La méthode par défaut pour l'authentification et l'autorisation utilise les coordonnées de connexion de l'utilisateur.

- Authentification
  - Activé par le paramètre du groupe de serveurs d'authentification dans le groupe de tunnels (également appelé profil de connexion ASDM)
  - Utilise le nom d'utilisateur et le mot de passe comme identifiant
- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation dans le groupe de tunnels (également appelé profil de connexion ASDM)
  - Utilise le nom d'utilisateur comme identifiant

Certificats

Si des certificats numériques d'utilisateur sont configurés, l'ASA valide d'abord le certificat. Cependant, il n'utilise aucun des DN des certificats comme nom d'utilisateur pour l'authentification.

Si l'authentification et l'autorisation sont toutes deux activées, l'ASA utilise les coordonnées de connexion de l'utilisateur pour l'authentification et l'autorisation de l'utilisateur.

- Authentification
  - Activé par le paramètre du groupe de serveurs d'authentification
  - Utilise le nom d'utilisateur et le mot de passe comme identifiant
- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation
  - Utilise le nom d'utilisateur comme identifiant

Si l'authentification est désactivée et que l'autorisation est activée, l'ASA utilise le champ DN principal pour l'autorisation.

- Authentification
  - DÉSACTIVÉ (défini sur Aucun) par le paramètre du groupe de serveurs d'authentification
  - Aucun identifiant utilisé

- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation
  - Utilise la valeur du nom d'utilisateur du champ DN principal du certificat comme identifiant

Remarque Si le champ de DN principal n'est pas présent dans le certificat, l'ASA utilise la valeur du champ DN secondaire comme nom d'utilisateur pour la demande d'autorisation.

Prenons par exemple un certificat d'utilisateur qui comprend les champs et les valeurs de DN du sujet suivants :

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

Si le DN principal = EA (adresse courriel) et le DN secondaire = CN (nom commun), le nom d'utilisateur utilisé dans la demande d'autorisation serait anyuser@example.com.

Lignes directrices pour les certificats numériques

Cette section comprend des lignes directrices et des limites que vous devez vérifier avant de configurer les certificats numériques.

Directives relatives au mode contextuel

- Pris en charge en mode de contexte unique seulement pour les autorités de certification tierces.

Directives en matière de basculement

- Ne prend pas en charge la réplication des sessions dans le basculement dynamique.
- Ne prend pas en charge le basculement pour les autorités de certification locales.
- Les certificats sont automatiquement copiés sur l'unité de secours si vous configurez le basculement dynamique. Si vous constatez qu'un certificat est manquant, utilisez la commande **write standby** sur l'unité active.

Directives IPv6

Ne prend pas en charge IPv6.

Certificats de CA locale

- Assurez-vous que l'ASA est configuré correctement pour prendre en charge les certificats. Un ASA mal configuré peut entraîner l'échec de l'inscription ou demander un certificat contenant des renseignements inexacts.
- Assurez-vous que le nom d'hôte et le nom de domaine de l'ASA sont configurés correctement. Pour afficher le nom d'hôte et le nom de domaine actuellement configurés, saisissez la commande **show running-config**.

- Assurez-vous que l'horloge ASA est réglée avec précision avant de configurer la CA. Les certificats ont une date et une heure de validité et d'expiration. Lorsque l'ASA s'inscrit auprès d'une CA et obtient un certificat, l'ASA vérifie que l'heure actuelle se situe dans la plage de validité du certificat. Si ce n'est pas le cas, l'inscription échoue.
- Trois jours avant l'expiration du certificat de CA locale, un certificat de renouvellement de remplacement est généré et un message de journal système informe l'administrateur qu'il est temps de procéder au renouvellement du certificat de CA locale. Le nouveau certificat de CA locale doit être importé sur tous les périphériques nécessaires avant l'expiration du certificat actuel. Si l'administrateur ne répond pas en installant le certificat de renouvellement comme nouveau certificat de CA locale, les validations peuvent échouer.
- Le certificat de CA locale est renouvelé automatiquement après son expiration en utilisant la même paire de clés. Le certificat de renouvellement peut être exporté au format base 64.

  L'exemple suivant montre un certificat de CA locale codé en base 64 :

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

Prise en charge du mandataire SCEP

- Assurez-vous que l'ASA et les nœuds de service de politique Cisco ISE sont synchronisés à l'aide du même serveur NTP.
- Secure Client (services client sécurisés) 3.0 ou une version ultérieure doit être en cours d'exécution sur le terminal.
- La méthode d'authentification, configurée dans le profil de connexion pour votre stratégie de groupe, doit être définie pour utiliser à la fois AAA et l'authentification par certificat.
- Un port SSL doit être ouvert pour les connexions VPN IKEv2.
- La CA doit être en mode d'octroi automatique.

Directives supplémentaires

- Le type de certificat que vous pouvez utiliser est limité par les types de certificats pris en charge par les applications qui utiliseront le certificat. Les certificats RSA sont généralement pris en charge par toutes les applications qui utilisent des certificats. Cependant, les certificats EDDSA peuvent ne pas être pris en charge par les systèmes d'exploitation des ordinateurs, les navigateurs, ASDM ou Secure Client (services client sécurisés). Par exemple, vous devez utiliser un certificat RSA pour l'identité et l'authentification VPN d'accès à distance. Pour le VPN de site à site, où l'ASA est l'application qui utilise le certificat, EDDSA est pris en charge.
- Pour les ASA configurés en tant que serveurs ou clients CA, limitez la période de validité du certificat à une date antérieure à la date de fin recommandée, soit le 19 janvier 2038 à 03:14:08 UTC. Ces lignes directrices s'appliquent également aux certificats importés de fournisseurs tiers.

- L'ASA établit une connexion LDAP/SSL uniquement si l'un des critères de certification suivants est satisfait :
  - Le certificat du serveur LDAP est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA) et est valide.
  - Un certificat d'autorité de certification des serveurs émettant la chaîne est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA), et tous les certificats d'autorité de certification subordonnés de la chaîne sont complets et valides.
- Lorsqu'une inscription de certificat est terminée, l'ASA stocke un fichier PKCS12 contenant la paire de clés et la chaîne de certificat de l'utilisateur, ce qui nécessite environ 2 Ko de mémoire flash ou d'espace disque par inscription. La quantité réelle d'espace disque dépend de la configuration de la clé RSA et des champs de certificat. Gardez ces lignes directrices à l'esprit lors de l'ajout d'un grand nombre d'inscriptions de certificat en attente sur un ASA avec une quantité limitée de mémoire flash disponible, car ces fichiers PKCS12 sont stockés dans la mémoire flash pendant toute la durée du délai d'expiration de récupération de l'inscription configuré. Nous vous conseillons d'utiliser une taille de clé d'au moins 2048.
- Vous devez configurer l'ASA pour utiliser un certificat d'identité afin de protéger le trafic ASDM et le trafic HTTPS vers l'interface de gestion. Les certificats d'identité qui sont automatiquement générés avec SCEP sont régénérés après chaque redémarrage, alors assurez-vous d'installer manuellement vos propres certificats d'identité. Pour obtenir un exemple de cette procédure qui s'applique uniquement à SSL, consultez l'URL suivante : http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml.
- L'ASA et le Secure Client (services client sécurisés) ne peuvent valider que les certificats dans lesquels le champ X520Serialnumber (numéro de série dans le nom d'objet) est au format PrintableString. Si le format du numéro de série utilise un encodage tel que UTF8, l'autorisation de certificat échouera.
- Utilisez uniquement des caractères et des valeurs valides pour les paramètres de certificat lorsque vous les importez sur l'ASA. Dans l'ASA, ces certificats sont décodés afin d'être intégrés dans des structures de données internes. Les certificats comportant des champs vides sont interprétés comme non conformes aux normes de décodage et, par conséquent, la validation de l'installation échoue. Cependant, à partir de la version 9.16, les valeurs vides des champs facultatifs n'ont aucune incidence sur les critères de décodage et de validation d'installation.
- Pour utiliser un caractère générique (*), assurez-vous d'utiliser l'encodage sur le serveur CA qui autorise ce caractère dans la valeur de chaîne. Bien que la RFC 5280 recommande d'utiliser un UTF8String ou PrintableString, vous devez utiliser UTF8String, car PrintableString ne reconnaît pas le caractère générique comme un caractère valide. L'ASA rejette le certificat importé si un caractère ou une valeur non valide est détecté pendant l'importation. Par exemple :

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H÷ytes
 as CA certificate:0U0= \Ivr"phÕv°3é¼p0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
 mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

Configurer les certificats numériques

Après avoir établi des certificats de confiance, vous pouvez commencer d'autres tâches fondamentales telles que l'établissement de certificats d'identité ou des configurations plus avancées telles que l'établissement de certificats de signature de code.

Avant de commencer

Lisez les renseignements sur les certificats numériques et établissez des certificats de confiance. Les certificats CA sans clé privée sont utilisés par tous les protocoles VPN, et sont configurés dans des points de confiance pour valider les certificats clients entrants.

Procédure

Étape 1 Un certificat d'identité est un certificat configuré sur l'ASA avec une clé privée correspondante. Il est utilisé pour le chiffrement sortant ou pour la génération de signatures lors de l'activation des services SSL et IPsec sur l'ASA et est obtenu par l'inscription du point de confiance. Pour configurer les certificats d'identité, consultez Configuration des certificats d'identité, à la page 814.

Étape 2 Pour configurer les CA, consultez Configuration des certificats CA, à la page 822.

Prochaine étape

Configurez une alerte d'expiration de certificat ou surveillez les certificats numériques et l'historique de gestion des certificats.

Configuration des certificats d'identité

Un certificat d'identité peut être utilisé pour authentifier l'accès VPN par l'ASA.

Dans le volet Identity Certificates Authentication (Authentification par certificats d'identité), vous pouvez effectuer les tâches suivantes :

- Ajouter ou importer un certificat d'identité, à la page 815.
- Activer les inscriptions CMPv2 à la demande d'une CA
- Afficher les détails d'un certificat d'identité.
- Supprimer un certificat d'identité existant.
- Exporter un certificat d'identité, à la page 819.
- Définir des alertes d'expiration de certificat.
- Vous inscrire pour un certificat d'identité avec Entrust Générer une requête de signature de certificat, à la page 820.

Ajouter ou importer un certificat d'identité

Pour ajouter ou importer une nouvelle configuration de certificat d'identité, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add Identity Certificate** (Ajouter un certificat d'identité) apparaît, avec le nom du point de confiance sélectionné affiché en haut.

Étape 3 Cliquez sur le bouton radio **Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)** (Importer le certificat d'identité à partir d'un fichier (format PKCS12 avec certificat(s) + clé privée)) pour importer un certificat d'identité à partir d'un fichier existant.

Étape 4 Entrez la phrase secrète utilisée pour déchiffrer le fichier PKCS12.

Étape 5 Saisissez le nom du chemin d'accès au fichier ou cliquez sur **Browse** (Parcourir) pour afficher la boîte de dialogue **Import ID Certificate File** (Importer le fichier de certificat d'ID). Recherchez le fichier de certificat, puis cliquez sur **Import ID Certificate File** (Importer le fichier de certificat d'ID).

Étape 6 Cliquez sur le bouton radio **Add a new identity certificate** (Ajouter un nouveau certificat d'identité) pour ajouter un nouveau certificat d'identité.

Étape 7 Cliquez sur **New** (Nouveau) pour afficher la boîte de dialogue **Add Key Pair** (Ajouter une paire de clés).

Étape 8 Choisissez le type de clé **RSA**, **ECDSA** ou **EdDSA**.

Étape 9 Si vous choisissez **EdDSA**, l'option **Edwards Curve** (Courbe d'Edwards) s'affiche. Cliquez sur le bouton radio EdDSA1.

Étape 10 Cliquez sur le bouton radio **Use default keypair name** (Utiliser le nom de la paire de clés par défaut) pour utiliser le nom de la paire de clés par défaut.

Étape 11 Cliquez sur le bouton radio **Enter a new key pair name** (Entrer un nouveau nom de paire de clés), puis saisissez le nouveau nom.

Étape 12 Choisissez la taille du module partir de la liste déroulante. Si **Edwards Curve** (Courbe d'Edwards) est sélectionné, choisissez Ed25519. Si vous n'êtes pas sûr de la taille du module, consultez Entrust.

Pour ASA 9.16(1) et les versions ultérieures, assurez-vous de sélectionner une taille de module RSA de 2 048 ou plus. La validation du certificat CA échoue lorsque la taille de la clé RSA est inférieure à 2 048 bits. Pour remplacer cette restriction, activez l'option d'autorisation de chiffrement faible. (Voir Autoriser le chiffrement faible pour les certificats CA, à la page 829).

Étape 13 Choisissez l'utilisation de la paire de clés en cliquant sur le bouton radio **General purpose** (Usage général) (par défaut) ou **Special** (Spécial). Lorsque vous choisissez le bouton radio **Special** (Spécial), l'ASA génère deux paires de clés, une pour la signature et une pour le chiffrement. Cette sélection indique que deux certificats sont requis pour l'identité correspondante.

Étape 14 Cliquez sur **Generate Now** (Générer maintenant) pour créer de nouvelles paires de clés, puis cliquez sur **Show** (Afficher) pour afficher la boîte de dialogue **Key Pair Details** (Détails de la paire de clés), qui contient les informations d'affichage uniquement :

- Le nom de la paire de clés dont la clé publique doit être certifiée.
- L'heure et la date auxquelles la paire de clés est générée.

- L'utilisation d'une paire de clés RSA.
- La taille du module (bits) des paires de clés : 512, 768, 1 024, 2 048, 3 072 et 4 096. La valeur par défaut est 2 048.
- Les données de clé, qui comprennent les données de clé spécifiques au format texte.

Étape 15 Cliquez sur **OK** lorsque vous avez terminé.

Étape 16 Choisissez un DN de sujet de certificat pour former le DN dans le certificat d'identité, puis cliquez sur **Select** (Sélectionner) pour afficher la boîte de dialogue **Certificate Subject DN** (DN du sujet du certificat).

Étape 17 Choisissez un ou plusieurs attributs de DN que vous souhaitez ajouter dans la liste déroulante, saisissez une valeur, puis cliquez sur **Add** (Ajouter). Les attributs X.500 disponibles pour le DN du sujet de certificat sont les suivants :

- **Nom usuel**
- **Service (OU)**
- **Nom de la société (O)**
- **Pays (C)**
- **État/Province (ST)**
- **Emplacement (L)**
- **Adresses de courriel (EA)**

Étape 18 Cliquez sur **OK** lorsque vous avez terminé.

Étape 19 Cochez la case **Generate self-signed certificate** (Générer un certificat autosigné) pour créer des certificats autosignés.

Étape 20 Cochez la case **Act as local certificate authority and issue dynamic certificates to TLS proxy** (Agir en tant qu'autorité de certification locale et émettre des certificats dynamiques au mandataire TLS) pour que le certificat d'identité agisse en tant qu'autorité CA locale.

Étape 21 Cliquez sur **Advanced** (Avancé) pour établir des paramètres de certificat d'identité supplémentaires.

La boîte de dialogue **Advanced Options** (Options avancées) apparaît, avec les trois onglets suivants : **Certificate Parameters** (Paramètres de certificat), **Enrollment Mode** (Mode d'inscription) et **SCEP Challenge Password** (Mot de passe du défi SCEP).

Remarque Les paramètres du mode d'inscription et le mot de passe du défi SCEP ne sont pas disponibles pour les certificats autosignés.

Étape 22 Cliquez sur l'onglet **Certificate Parameters** (Paramètres de certificat), puis saisissez les renseignements suivants :

- Le FQDN, un nom de domaine non ambivalent, pour indiquer la position du nœud dans la hiérarchie DNS.
- L'adresse courriel associée au certificat d'identité.
- L'adresse IP de l'ASA sur le réseau en notation décimale à quatre parties séparées par des points.

- Cochez la case **Include serial number of the device** (Inclure le numéro de série du périphérique) pour ajouter le numéro de série de l'ASA aux paramètres de certificat.

Étape 23 Cliquez sur l'onglet **Enrollment Mode** (Mode d'inscription), puis saisissez les renseignements suivants :

- Choisissez la méthode d'inscription en cliquant sur le bouton radio **Request by manual enrollment** (Demande par inscription manuelle) ou sur le bouton radio **Request from a CA** (Demande d'une autorité de certification). Si vous choisissez **Request from a CA** (Demande d'une autorité de certification), pour en savoir plus sur l'activation des inscriptions CMPV2, consultez Activer les inscriptions CMPv2 à la demande d'une CA , à la page 818.
- Choisissez le protocole d'inscription : scep, cmp, ou est.

Remarque Seules les clés RSA et ECDSA sont prises en charge pour l'inscription de certificat CMP .

- L'URL d'inscription du certificat à installer automatiquement par le biais de SCEP.
- Le nombre maximum de minutes autorisées pour réessayer d'installer un certificat d'identité. La valeur par défaut est d'une minute.
- Le nombre maximum de tentatives autorisées pour l'installation d'un certificat d'identité. La valeur par défaut est zéro, ce qui indique un nombre illimité de tentatives dans la période de réessai.

Étape 24 Cliquez sur l'onglet **SCEP Challenge Password** (Mot de passe du défi SCEP), puis saisissez les renseignements suivants :

- Le mot de passe SCEP
- La confirmation du mot de passe SCEP

Étape 25 Cliquez sur **OK** lorsque vous avez terminé.

Étape 26 Cochez la case **Enable CA flag in basic constraints extension** (Activer l'indicateur de CA dans l'extension de contraintes de base) si ce certificat doit être en mesure de signer d'autres certificats.

L'extension des contraintes de base détermine si le sujet du certificat est une autorité de certification (CA), auquel cas le certificat peut être utilisé pour signer d'autres certificats. L'indicateur de d'autorité de certification fait partie de cette extension. La présence de ces éléments dans un certificat indique que la clé publique du certificat peut être utilisée pour valider les signatures de certificat. Il n'y a aucun mal à laisser cette option sélectionnée.

Étape 27 Cliquez sur **Add Certificate** (Ajouter un certificat) dans la boîte de dialogue **Add Identity Certificate** (Ajouter un certificat d'identité).

Le nouveau certificat d'identité apparaît dans la liste des certificats d'identité.

Étape 28 Cliquez sur **Apply** (Appliquer) pour enregistrer la configuration du nouveau certificat d'identité.

Étape 29 Cliquez sur **Show Details** (Afficher les détails) pour afficher la boîte de dialogue **Certificate Details** (Détails du certificat), qui comprend les trois onglets d'affichage uniquement suivants :

- L'onglet **General** (Général) affiche les valeurs pour le type, le numéro de série, l'état, l'utilisation, le type de clé publique, le point de distribution de la CRL, les délais de validité du certificat et les points de confiance associés. Les valeurs s'appliquent à l'état disponible et à l'état en attente.
- L'onglet **Issued to** (Émis pour) affiche les champs X.500 du DN du sujet ou du propriétaire du certificat visé ainsi que leurs valeurs. Les valeurs s'appliquent uniquement à l'état disponible.
- L'onglet **Issued by** (Émis par) affiche les champs X.500 de l'entité qui accorde le certificat. Les valeurs s'appliquent uniquement à l'état disponible.

Étape 30 Pour supprimer une configuration de certificat d'identité, sélectionnez-la, puis cliquez sur **Delete** (Supprimer).

Remarque Après avoir supprimé une configuration de certificat, elle ne peut pas être restaurée. Pour recréer le certificat supprimé, cliquez sur **Add** (Ajouter) pour saisir à nouveau tous les renseignements de configuration du certificat.

Activer les inscriptions CMPv2 à la demande d'une CA

Pour être placé en tant qu'appareil de passerelle de sécurité dans les réseaux LTE sans fil, l'ASA prend en charge certaines fonctions de gestion des certificats à l'aide du protocole de gestion des certificats (CMPv2). En utilisant CMPv2 pour l'inscription de certificats de périphérique ASA, vous pouvez effectuer l'inscription manuelle, pour le certificat principal et secondaire de l'autorité de certification compatible avec CMPv2, ou des mises à jour de certificat manuelles, pour le remplacement d'un certificat précédemment émis à l'aide de la même paire de clés. Les certificats reçus sont stockés en dehors de la configuration traditionnelle et sont utilisés dans les configurations IPsec compatibles avec les certificats.

Remarque Vous n'aurez pas la fonctionnalité CMPv2 complète sur l'ASA.

Une demande initiale établit la confiance avec l'autorité de certification et obtient le premier certificat. Un certificat CA doit être préconfiguré dans un point de confiance. L'authentification a lieu lorsque vous reconnaissez l'empreinte digitale du certificat installé.

Après avoir cliqué sur **Request from a CA** (Demande d'une autorité de certification) dans l'onglet Enrollment Mode (Mode d'inscription) de la fenêtre Advanced Options (Options avancées), procédez comme suit pour les inscriptions CMPv2 :

Avant de commencer

- Suivez les étapes dans Ajouter ou importer un certificat d'identité, à la page 815.
- La licence de l'opérateur doit être incluse pour permettre l'inscription au CMP.

Procédure

Étape 1 Choisissez CMP comme protocole d'inscription et saisissez l'URL du CMP dans la zone http://.

Étape 2 Pour générer automatiquement de nouvelles paires de clés pour toutes les inscriptions CMP manuelles et automatiques, choisissez **RSA** ou **EDCSA**.

Si vous choisissez RSA, choisissez une valeur dans le menu déroulant Modules. Si vous choisissez EDCSA, choisissez une valeur dans le menu déroulant elliptic-curve (courbe elliptique).

Étape 3 (Facultatif) Cliquez sur **Regenerate the key pair** (Régénérer la paire de clés) pour générer une paire de clés lors du renouvellement du certificat ou avant de créer la demande d'inscription.

Étape 4 Cliquez sur **Shared Key** (Clé partagée) et saisissez une valeur fournie hors bande par la CA. Cette valeur est utilisée par la CA et l'ASA pour confirmer l'authentificité et l'intégrité des messages qu'ils échangent.

Étape 5 Cliquez sur **Signing Trustpoint** (Point de confiance de signature) et entrez le nom du point de confiance qui contient un certificat d'appareil émis précédemment utilisé pour signer la demande d'inscription au CMP.

Ces options ne sont disponibles que lorsque le protocole d'inscription auprès du point de confiance est défini sur CMP. Lorsqu'il s'agit d'un point de confiance CMP, le secret partagé ou le certificat de signature peut être spécifié, mais pas les deux.

Étape 6 Cliquez sur **Browse Certificate** (Parcourir le certificat) pour spécifier le certificat CA.

Étape 7 (Facultatif) Cliquez sur la case **Auto Enroll** (Inscription automatique) pour déclencher l'inscription automatique de CMPv2.

Étape 8 Dans le champ Auto Enroll Lifetime (Durée de vie de l'inscription automatique), saisissez le pourcentage de la durée de vie absolue du certificat après lequel l'inscription automatique sera nécessaire.

Étape 9 Cliquez sur **Auto Enroll Regenerate Key** (Regénérer la clé pour l'inscription automatique) pour regénérer une nouvelle clé lors du renouvellement du certificat.

Exporter un certificat d'identité

Pour exporter un certificat d'identité, procédez comme suit :

Procédure

Étape 1 Cliquez sur **Export** (Exporter) pour afficher la boîte de dialogue **Export Certificate** (Exporter le certificat).

Étape 2 Saisissez le nom du fichier de format PKCS12 à utiliser pour exporter la configuration du certificat. Sinon, cliquez sur **Browse** (Parcourir) pour afficher la boîte de dialogue **Export ID Certificate File** (Exporter le fichier de certificat d'ID) pour trouver le fichier vers lequel vous souhaitez exporter la configuration du certificat.

Étape 3 Choisissez le format de certificat en cliquant sur le bouton radio **PKCS12 Format** (Format PKCS12) ou le bouton radio **PEM Format** (Format PEM).

Étape 4 Entrez la phrase secrète utilisée pour chiffrer le fichier PKCS12 pour l'exportation.

Étape 5 Confirmez la phrase secrète de chiffrement.

Étape 6 Cliquez sur **Export Certificate** (Exporter le certificat) pour exporter la configuration du certificat.

Une boîte de dialogue d'information s'affiche et vous informe que le fichier de configuration du certificat a été exporté avec succès vers l'emplacement que vous avez spécifié.

Générer une requête de signature de certificat

Pour générer une requête de signature de certificat à envoyer à EnTrust, procédez comme suit :

Procédure

Étape 1 Cliquez sur **Enroll ASA SSL VPN with Entrust** (Enregistrer ASA SSL VPN auprès d'Entrust) pour afficher la boîte de dialogue **Generate Certificate Signing Request** (Générer une requête de signature de certificat).

Étape 2 Exécutez les étapes suivantes dans la zone **Key Pair** (Paire de clés) :

a) Choisissez l'une des paires de clés configurées dans la liste déroulante.
b) Cliquez sur **Show** (Afficher) pour afficher la boîte de dialogue **Key Details** (Détails de la clé), qui fournit des renseignements sur la paire de clés sélectionnée, y compris la date et l'heure de génération, l'utilisation (générale ou spéciale), la taille du module et les données de la clé.
c) Cliquez sur **OK** lorsque vous avez terminé.
d) Cliquez sur **New** (Nouveau) pour afficher la boîte de dialogue **Add Key Pair** (Ajouter une paire de clés). Lorsque vous générez la paire de clés, vous pouvez l'envoyer à l'ASA ou l'enregistrer dans un fichier.

Étape 3 Saisissez les renseignements suivants dans le champ **Certificate Subject DN** (DN du sujet du certificat) :

a) Le FQDN ou l'adresse IP de l'ASA.
b) Le nom de l'entreprise.
c) Le code pays à deux lettres.

Étape 4 Effectuez les étapes suivantes dans la zone **Optional Parameters** (Paramètres facultatifs) :

a) Cliquez sur **Select** (Sélectionner) pour afficher la boîte de dialogue **Additional DN Attributes** (Attributs de DN supplémentaires).
b) Choisissez l'attribut à ajouter dans la liste déroulante, puis saisissez une valeur.
c) Cliquez sur **Add** (Ajouter) pour ajouter chaque attribut au tableau d'attributs.
d) Cliquez sur **Delete** (Supprimer) pour supprimer un attribut du tableau d'attributs.
e) Cliquez sur **OK** lorsque vous avez terminé.

Les attributs ajoutés apparaissent dans le champ **Additional DN Attributes** (Attributs de DN supplémentaires).

Étape 5 Saisissez des renseignements supplémentaires sur le nom de domaine complet si la CA le demande.

Étape 6 Cliquez sur **Generate Request (**Générer la demande) pour générer la requête de signature de certificat, que vous pouvez ensuite envoyer à Entrust ou enregistrer dans un fichier et envoyer ultérieurement.

La boîte de dialogue **Enroll with Entrust** (S'inscrire auprès d'Entrust) apparaît, avec la CSR.

Étape 7 Terminez le processus d'inscription en cliquant sur le lien **request a certificate from Entrust** (demande de certificat auprès d'Entrust). Copiez et collez ensuite la CSR fournie et soumettez-la à l'aide du formulaire web Entrust, fourni à l'adresse http://www.entrust.net/cisco/. Sinon, pour vous inscrire ultérieurement, enregistrez la CSR générée dans un fichier, puis cliquez sur le lien **enroll with Entrust** (s'inscrire auprès d'Entrust) dans le volet **Identity Certificates** (Certificats d'identité).

Étape 8 Entrust émet un certificat après avoir vérifié l'authentification de votre demande, ce qui peut prendre plusieurs jours. Vous devez ensuite installer le certificat en sélectionnant la demande en attente dans le volet **Identity Certificate** (Certificat d'identité) et en cliquant sur **Install** (Installer).

Étape 9 Cliquez sur **Close** (Fermer) pour fermer la boîte de dialogue **Enroll with Entrust** (S'inscrire auprès d'Entrust).

Installer des certificats d'identité

Pour installer un nouveau certificat d'identité, procédez comme suit :

Procédure

Étape 1 Cliquez sur **Add** (Ajouter) dans le volet **Identity Certificates** (Certificats d'identité) pour afficher la boîte de dialogue **Add Identity Certificate** (Ajouter un certificat d'identité).

Étape 2 Cliquez sur le bouton radio **Add a new identity certificate** (Ajouter un nouveau certificat d'identité).

Étape 3 Modifiez la paire de clés ou créez-en une nouvelle. Une paire de clés est requise.

Étape 4 Saisissez les renseignements sur le DN du sujet du certificat, puis cliquez sur **Select** (Sélectionner) pour afficher la boîte de dialogue **Certificate Subject DN** (DN du sujet du certificat).

Étape 5 Spécifiez tous les attributs de DN du sujet requis par la CA concernée, puis cliquez sur **OK** pour fermer la boîte de dialogue **Certificate Subject DN** (DN du sujet du certificat).

Étape 6 Dans la boîte de dialogue **Add Identity Certificate** (Ajouter un certificat d'identité), cliquez sur **Advanced** (Avancé) pour afficher la boîte de dialogue **Advanced Options** (Options avancées).

Étape 7 Pour continuer, consultez les étapes 17 à 23 de Ajouter ou importer un certificat d'identité, à la page 815.

Étape 8 Dans la boîte de dialogue **Add Identity Certificate** (Ajouter un certificat d'identité), cliquez sur **Add Certificate** (Ajouter un certificat).

La boîte de dialogue **Identity Certificate Request** (Demande de certificat d'identité) apparaît.

Étape 9 Saisissez le nom de fichier CSR du type, du texte, tel que c:\verisign-csr.txt, puis cliquez sur **OK**.

Étape 10 Envoyez le fichier texte CSR à la CA. Vous pouvez également coller le fichier texte dans la page d'inscription à la CSR sur le site Web de la CA.

Étape 11 Lorsque la CA vous renvoie le certificat d'identité, accédez au volet **Identity Certificates** (Certificats d'identité), sélectionnez l'entrée de certificat en attente, puis cliquez sur **Install** (Installer).

La boîte de dialogue **Install Identity Certificate** (Installer le certificat d'identité) apparaît.

Étape 12 Choisissez l'une des options suivantes en cliquant sur le bouton radio applicable :

- **Install from a file** (Installer à partir d'un fichier).

  Sinon, cliquez sur **Browse** (Parcourir) pour rechercher le fichier.

- **Paste the certificate data in base-64 format** (Coller les données de certificat au format base-64).

  Collez les données de certificat copiées dans la zone fournie.

Étape 13 Cliquez sur **Install Certificate** (Installer le certificat).

Étape 14 Cliquez sur **Apply** (Appliquer) pour enregistrer le certificat nouvellement installé avec la configuration ASA.

Étape 15 Pour afficher des renseignements détaillés sur le certificat d'identité sélectionné, cliquez sur **Show Details** (Afficher les détails) pour afficher la boîte de dialogue **Certificate Details** (Détails du certificat), qui comprend les trois onglets d'affichage uniquement suivants :

L'onglet **General** (Général) affiche les valeurs pour le type, le numéro de série, l'état, l'utilisation, le type de clé publique, le point de distribution de la CRL, les délais de validité du certificat et les points de confiance associés. Les valeurs s'appliquent à l'état disponible et à l'état en attente.

L'onglet **Issued to** (Émis pour) affiche les champs X.500 du DN du sujet ou du propriétaire du certificat visé ainsi que leurs valeurs. Les valeurs s'appliquent uniquement à l'état disponible.

L'onglet **Issued by** (Émis par) affiche les champs X.500 de l'entité qui accorde le certificat. Les valeurs s'appliquent uniquement à l'état disponible.

Étape 16 Pour supprimer une configuration de certificat de signataire de code, sélectionnez-la, puis cliquez sur **Delete** (Supprimer).

Remarque Après avoir supprimé une configuration de certificat, elle ne peut pas être restaurée. Pour recréer le certificat supprimé, cliquez sur **Import** (Importer) pour saisir à nouveau tous les renseignements de configuration du certificat.

Configuration des autorités de certification

Configuration des certificats CA

Cette page vous permet de gérer les certificats CA. Les rubriques suivantes expliquent ce que vous pouvez faire.

Ajouter ou installer un certificat CA

Pour ajouter ou installer un certificat CA, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue **Install Certificate** (Installer le certificat) s'affiche.

Étape 3 Cliquez sur le bouton radio **Install from a file** (Installer à partir d'un fichier) pour ajouter une configuration de certificat à partir d'un fichier existant (il s'agit du paramètre par défaut).

Étape 4 Saisissez le chemin d'accès et le nom du fichier, ou cliquez sur **Browse** (Parcourir) pour rechercher le fichier. Cliquez ensuite sur **Install Certificate** (Installer le certificat).

Étape 5 La boîte de dialogue **Certificate Installation** (Installation du certificat) s'affiche avec un message de confirmation indiquant que le certificat a été installé avec succès. Cliquez sur **OK** pour fermer cette boîte de dialogue.

Étape 6 Cliquez sur le bouton radio **Paste certificate in PEM format** (Coller le certificat dans le format PEM) pour vous inscrire manuellement.

Étape 7 Copiez et collez le certificat au format PEM (base64 ou hexadécimal) dans la zone fournie, puis cliquez sur **Install Certificate** (Installer le certificat).

Étape 8 La boîte de dialogue **Certificate Installation** (Installation du certificat) s'affiche avec un message de confirmation indiquant que le certificat a été installé avec succès. Cliquez sur **OK** pour fermer cette boîte de dialogue.

Étape 9 Cliquez sur le bouton radio **Use SCEP** (Utiliser SCEP) pour l'inscription automatique. L'ASA communique avec la CA à l'aide de SCEP, obtient les certificats et les installe sur le périphérique. Pour utiliser SCEP, vous devez vous inscrire auprès d'une CA qui prend en charge SCEP et vous devez vous inscrire par Internet. L'inscription automatique à l'aide de SCEP nécessite que vous fournissiez les renseignements suivants :

- Le chemin d'accès et le nom de fichier du certificat à installer automatiquement.
- Le nombre maximum de minutes pour réessayer l'installation du certificat. La valeur par défaut est d'une minute.
- Le nombre de tentatives d'installation d'un certificat. La valeur par défaut est zéro, ce qui indique un nombre illimité de tentatives dans la période de réessai.

Étape 10 Cliquez sur **More Options** (Plus d'options) pour afficher des options de configuration supplémentaires pour les nouveaux certificats et les certificats existants.

Le volet **Configuration Options for CA Certificates** (Options de configuration des certificats CA) apparaît.

Étape 11 Pour modifier la configuration d'un certificat CA existant, sélectionnez-le, puis cliquez sur **Edit** (Modifier).

Étape 12 Pour supprimer la configuration d'un certificat CA, sélectionnez-le, puis cliquez sur **Delete** (Supprimer).



Remarque Après avoir supprimé une configuration de certificat, elle ne peut pas être restaurée. Pour recréer le certificat supprimé, cliquez sur **Add** (Ajouter) pour saisir à nouveau tous les renseignements de configuration du certificat.

Étape 13 Cliquez sur **Show Details** (Afficher les détails) pour afficher la boîte de dialogue **Certificate Details** (Détails du certificat), qui comprend les trois onglets d'affichage uniquement suivants :

- L'onglet **General** (Général) affiche les valeurs pour le type, le numéro de série, l'état, l'utilisation, le type de clé publique, le point de distribution de la CRL, les délais de validité du certificat et les points de confiance associés. Les valeurs s'appliquent à l'état disponible et à l'état en attente.
- L'onglet **Issued to** (Émis pour) affiche les champs X.500 du DN du sujet ou du propriétaire du certificat visé ainsi que leurs valeurs. Les valeurs s'appliquent uniquement à l'état disponible.
- L'onglet **Issued by** (Émis par) affiche les champs X.500 de l'entité qui accorde le certificat. Les valeurs s'appliquent uniquement à l'état disponible.

Configurer les certificats CA pour la révocation

Pour configurer les certificats CA pour la révocation, procédez comme suit :

Procédure

Étape 1 Sélectionnez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)** > **Add (Ajouter)** pour afficher la boîte de dialogue **Install Certificates** (Installer les certificats). Cliquez sur **More Options** (Plus d'options).

Étape 2 Cliquez sur l'onglet **Revocation Check** (Vérification de la révocation).

Étape 3 Cliquez sur le bouton radio **Do not check certificates for revocation** (Ne pas vérifier les certificats pour la révocation) pour désactiver la vérification de la révocation des certificats.

Étape 4 Cliquez sur le bouton radio **Check certificates for revocation** (Vérifier les certificats pour la révocation) pour sélectionner une ou plusieurs méthodes de vérification de la révocation (CRL ou OCSP).

Étape 5 Cliquez sur **Add** (Ajouter) pour déplacer une méthode de révocation vers la droite et la rendre disponible. Cliquez sur **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas) pour modifier l'ordre des méthodes.

Les méthodes que vous choisissez sont mises en œuvre dans l'ordre dans lequel vous les ajoutez. Si une méthode renvoie une erreur, la méthode de vérification de la révocation suivante s'active.

Étape 6 Cochez la case **Consider certificate valid if revocation information cannot be retrieved (Considérer le certificat valide si les informations de révocation ne peuvent pas être récupérées)** pour ignorer les erreurs de vérification de la révocation lors de la validation du certificat.

Étape 7 Cliquez sur **OK** pour fermer l'onglet **Revocation Check** (Vérification de la révocation).

Configurer la politique de récupération des CRL

Pour configurer la politique de récupération des CRL, procédez comme suit :

Avant de commencer

- Pour attribuer des URL statiques :

Procédure

Étape 1 Sélectionnez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)** > **Add (Ajouter)** pour afficher la boîte de dialogue **Install Certificates** (Installer les certificats). Cliquez sur **More Options** (Plus d'options).

Étape 2 Cochez la case **Use CRL Distribution Point from the certificate** (Utiliser le point de distribution CRL du certificat) pour diriger la vérification de la révocation vers le point de distribution de la CRL à partir du certificat en cours de vérification.

Étape 3 Cochez la case **Use Static URLs configured below** (Utiliser les URL statiques configurées ci-dessous) pour répertorier les URL précises à utiliser pour la récupération des CRL. Les URL que vous sélectionnez sont mises en œuvre dans l'ordre dans lequel vous les ajoutez. Si une erreur se produit avec l'URL indiquée, l'URL suivante est prise dans l'ordre.

Étape 4 Cliquez sur **Add** (Ajouter) dans l'onglet la zone **Static Configuration** (Configuration statique).

La boîte de dialogue **Add Static URL** (Ajouter une URL statique) apparaît.

Étape 5 Saisissez l'URL statique à utiliser pour la distribution des CRL, puis cliquez sur **OK**.

L'URL que vous avez saisie apparaît dans la liste **Static URLs** (URL statiques).

Étape 6 Cliquez sur **OK** pour fermer cette boîte de dialogue.

Configurer les méthodes de récupération des CRL

Pour configurer les méthodes de récupération des CRL, procédez comme suit :

Procédure

Étape 1 Sélectionnez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)** > **Add (Ajouter)** pour afficher la boîte de dialogue **Install Certificates** (Installer les certificats). Cliquez sur **More Options** (Plus d'options).

Étape 2 Cliquez sur l'onglet **CRL Retrieval Methods** (Méthodes de récupération des CRL) dans le volet **Configuration Options for CA Certificates** (Options de configuration pour les certificats CA).

Étape 3 Choisissez l'une des trois méthodes de récupération suivantes :

- Pour activer LDAP pour la récupération des CRL, cochez la case **Enable Lightweight Directory Access Protocol (LDAP)** (Activer le protocole LDAP). Avec LDAP, la récupération des CRL démarre une session LDAP en se connectant à un serveur LDAP nommé, accessible par un mot de passe. La connexion s'effectue sur le port TCP 389 par défaut. Entrez les paramètres requis suivants :
  - **Nom**
  - **Mot de passe**
  - **Confirmer le mot de passe**
  - **Serveur par défaut** (nom du serveur)
  - **Port par défaut** (389)
- Pour activer HTTP pour la récupération des CRL, cochez la case **Enable HTTP** (Activer HTTP).

Étape 4 Cliquez sur **OK** pour fermer cet onglet.

Configurer les règles OCSP

Pour configurer les règles OCSP afin d'obtenir l'état de révocation d'un certificat numérique X.509, procédez comme suit.

Avant de commencer

Assurez-vous d'avoir configuré une carte de certificat avant d'essayer d'ajouter des règles OCSP. Si aucune carte de certificat n'a été configurée, un message d'erreur s'affiche.

Procédure

Étape 1 Sélectionnez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)** > **Add (Ajouter)** pour afficher la boîte de dialogue **Install Certificates** (Installer les certificats). Cliquez sur **More Options** (Plus d'options).

Étape 2 Cliquez sur l'onglet **OCSP Rules** (Règles OCSP) dans le volet **Configuration Options for CA Certificates** (Options de configuration pour les certificats CA).

Étape 3 Choisissez la carte de certificat à faire correspondre à cette règle OCSP. Les cartes de certificats correspondent aux autorisations des utilisateurs à des champs spécifiques d'un certificat. Le nom de la CA utilisée par l'ASA pour valider les certificats du répondeur apparaît dans le champ **Certificat** (Certificate). Le numéro de priorité de la règle apparaît dans le champ **Index**. L'URL du serveur OCSP pour ce certificat apparaît dans le champ **URL**.

Étape 4 Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add OCSP Rule** (Ajouter une règle OCSP) apparaît.

Étape 5 Sélectionnez le mappage de certificats à utiliser dans la liste déroulante.

Étape 6 Sélectionnez le certificat à utiliser dans la liste déroulante.

Étape 7 Saisissez le numéro de priorité de la règle.

Étape 8 Saisissez l'URL du serveur OCSP pour ce certificat.

Étape 9 Lorsque vous avez terminé, cliquez sur **OK** pour fermer cette boîte de dialogue.

La règle OCSP nouvellement ajoutée apparaît dans la liste.

Étape 10 Cliquez sur **OK** pour fermer cet onglet.

Configurer les paramètres avancés de la CRL et de l'OCSP

Pour configurer des paramètres CRL et OCSP supplémentaires, procédez comme suit :

Procédure

Étape 1 Sélectionnez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)** > **Add (Ajouter)** pour afficher la boîte de dialogue **Install Certificates** (Installer les certificats). Cliquez sur **More Options** (Plus d'options).

Étape 2 Cliquez sur l'onglet **Advanced** (Avancé) dans le volet **Configuration Options for CA Certificates** (Options de configuration pour les certificats CA).

Étape 3 Saisissez le nombre de minutes entre les actualisations du cache dans la zone **CRL Options** (Options CRL). La valeur par défaut est de 60 minutes. La plage autorisée est de 1 à 1440 minutes. Pour éviter d'avoir à récupérer la même CRL d'une autorité de certification à plusieurs reprises, l'ASA peut stocker les CRL extraites localement, ce qui s'appelle la mise en cache des CRL. La capacité du cache CRL varie selon la plateforme et est cumulative dans tous les contextes. Si une tentative de mise en cache d'une CRL nouvellement extraite dépassait ses limites de stockage, l'ASA supprime la CRL la moins récemment utilisée jusqu'à ce que plus d'espace se libère.

Étape 4 Cochez la case **Enforce next CRL update** (Appliquer la prochaine mise à jour de la CRL) pour exiger que les CRL valides aient une valeur de prochaine mise à jour qui n'a pas expiré. Décochez la case **Enforce next CRL update** (Appliquer la prochaine mise à jour de la CRL) pour laisser les CRL valides sans valeur de mise à jour suivante ou si la valeur de mise à jour suivante a expiré.

Étape 5 Saisissez l'URL du serveur OCSP dans le champ **OCSP Options** (Options OCSP). L'ASA utilise les serveurs OCSP selon l'ordre suivant :

a) URL OCSP dans une règle de remplacement de certificat de correspondance
b) URL OCSP configurée dans l'attribut OCSP Options (Options OCSP) sélectionné
c) Champ AIA d'un certificat d'utilisateur

Étape 6 Par défaut, la case **Disable nonce extension** (Désactiver l'extension de nonce) est cochée, ce qui lie cryptographiquement les requêtes aux réponses pour éviter les attaques par relecture. Ce processus fonctionne en faisant correspondre l'extension dans la demande à celle dans la réponse, en s'assurant qu'elles sont identiques. Décochez la case **Disable nonce extension** (Désactiver l'extension de nonce) si le serveur OCSP que vous utilisez envoie des réponses prégénérées qui n'incluent pas cette extension de nonce correspondante.

Étape 7 Choisissez l'une des options suivantes dans la zone **Other Options** (Autres options) :

- Cochez la case **Accept certificates issued by this CA** (Accepter les certificats émis par cette autorité de certification) pour indiquer que l'ASA doit accepter les certificats de la CA spécifiée.
- Cochez la case **Accept certificates issued by the subordinate CAs of this CA** (Accepter les certificats émis par les autorités de certification subordonnées de cette autorité de certification) pour indiquer que l'ASA doit accepter les certificats de la CA subordonnée.

Étape 8 Cliquez sur **OK** pour fermer cet onglet, puis cliquez sur **Apply** (Appliquer) pour enregistrer les modifications de votre configuration.

Gérer les certificats de l'utilisateur

Pour modifier l'état du certificat, procédez comme suit :

Procédure

Étape 1 Sélectionnez des certificats spécifiques par nom d'utilisateur ou par numéro de série de certificat dans le volet **Manage User Certificates** (Gérer les certificats d'utilisateur).

Étape 2 Choisissez une des options suivantes :

- Cliquez sur **Revoke** (Révoquer) pour supprimer l'accès utilisateur si la durée de validité du certificat utilisateur est expirée. La CA locale marque également le certificat comme révoqué dans la base de données des certificats, met automatiquement à jour les renseignements réémet la liste CRL.
- Sélectionnez un certificat révoqué et cliquez sur **Unrevoke** (Annuler la révocation) pour rétablir l'accès. La CA locale marque également le certificat comme non révoqué dans la base de données des certificats, met automatiquement à jour les renseignements du certificat et réémet une liste CRL mise à jour.

Étape 3 Cliquez sur **Apply** (Appliquer) lorsque vous avez terminé pour enregistrer vos modifications.

Configurer les identités de référence

Lorsque l'ASA agit en tant que client TLS, il prend en charge les règles de vérification de l'identité d'un serveur d'applications, comme défini dans la RFC 6125. Cette RFC spécifie les procédures pour représenter les identités de référence (configurées sur l'ASA) et les vérifier par rapport aux identités présentées (envoyées par le serveur d'applications). Si l'identité présentée ne peut pas être comparée à l'identité de référence configurée, la connexion n'est pas établie et une erreur est enregistrée.

Le serveur présente son identité en incluant un ou plusieurs identifiants dans le certificat de serveur présenté à l'ASA lors de l'établissement de la connexion. Les identités de référence sont configurées sur l'ASA pour être comparées à l'identité présentée dans un certificat de serveur lors de l'établissement de la connexion. Ces identifiants sont des instances spécifiques des quatre types d'identifiants spécifiés dans la RFC 6125. Les quatre types d'identifiants sont les suivants :

- CN_ID : nom distinctif relatif (RDN) dans un champ d'objet de certificat qui ne contient qu'une seule paire d'attributs types et de valeurs de type de nom commun (CN), dans lequel la valeur correspond à la forme globale d'un nom de domaine. La valeur CN ne peut pas être en texte libre. Un identifiant de référence CN-ID n'identifie pas un service d'application.
- DNS-ID : une entrée subjectAltName de type dNSName. Il s'agit d'un nom de domaine DNS. Un identifiant de référence DNS-ID n'identifie pas un service d'application.
- SRV-ID : une entrée subjectAltName de type otherName dont le format de nom est SRVName comme défini dans la RFC 4985. Un identifiant SRV-ID peut contenir à la fois un nom de domaine et un type de service d'application. Par exemple, un SRV-ID de « _imaps.example.net » serait divisé en une partie de nom de domaine DNS de « example.net » et une partie de type de service d'application de « imaps ».
- URI-ID : Une entrée subjectAltName de type uniformResourceIdentifier dont la valeur comprend à la fois (i) un schéma et (ii) un composant « hôte » (ou son équivalent) qui correspond à la règle « reg-name » spécifiée dans la RFC 3986. Un identifiant URI-ID doit contenir le nom de domaine DNS, pas l'adresse IP et pas seulement le nom d'hôte. Par exemple, un URI-ID de « sip:voice.example.edu » serait divisé en une partie de nom de domaine DNS de « voice.example.edu » et un type de service d'application de « sip ».

Une identité de référence est créée lors de la configuration d'une identité avec un nom précédemment inutilisé. Une fois qu'une identité de référence a été créée, les quatre types d'identifiants et leurs valeurs associées peuvent être ajoutés ou supprimés de l'identité de référence. Les identifiants de référence PEUVENT contenir des renseignements identifiant le service d'application et doivent contenir des renseignements identifiant le nom de domaine DNS.

Avant de commencer

- Les identités de référence sont utilisées lors de la connexion au serveur de journal système et au serveur de licences Smart uniquement. Aucune autre connexion en mode client SSL ASA ne prend actuellement en charge la configuration ou l'utilisation des identités de référence.
- L'ASA met en œuvre toutes les règles de correspondance des identifiants décrites dans la RFC 6125, à l'exception des certificats épinglés et du système de secours pour les clients interactifs.
- La possibilité d'épingler des certificats n'est pas mise en œuvre. Par conséquent, `aucune correspondance n'a été trouvée, le certificat épinglé` ne se produira pas. De plus, un utilisateur n'aura pas la possibilité d'épingler un certificat si aucune correspondance n'est trouvée, car notre mise en œuvre n'est pas un client interactif.

Procédure

Étape 1 Accédez à **Configuration > Remote Access VPN (VPN d'accès à distance) > Advanced (Avancé) > Reference Identity (Identité de référence)**.

Les identités de référence configurées sont répertoriées. Vous pouvez en **ajouter** une nouvelle, choisir et **modifier** une existante, ou choisir et **supprimer** une existante. Une identité de référence en cours d'utilisation ne peut pas être supprimée.

Étape 2 Créez ou modifiez les ID de référence en sélectionnant **Add** (Ajouter) ou **Edit** (Modifier).

Utilisez cette boîte de dialogue Add or Edit Reference Identity (Ajouter ou modifier l'identité de référence) pour choisir et préciser vos ID de référence.

- Plusieurs identifiants de référence de tout type peuvent être ajoutés à l'identité de référence.
- Vous ne pouvez pas modifier le nom une fois qu'il est défini, supprimer et recréer une identité de référence pour modifier le nom.

Prochaine étape

Utilisez l'identité de référence lors de la configuration des connexions du journal système et du serveur Smart Call Home.

Autoriser le chiffrement faible pour les certificats CA

Lorsque les attributs suivants sont présents, l'opération de validation du certificat CA échoue :

- Certificats signés avec le SHA-1 avec algorithme de chiffrement RSA.
- Certificats avec une taille de clé RSA inférieure à 2 048 bits.

Cependant, vous pouvez remplacer ces restrictions en configurant l'option d'autorisation de chiffrement faible. Lorsqu'elle est activée, l'ASA autorise l'utilisation des attributs ci-dessus lors de la validation des certificats. Nous déconseillons d'autoriser les clés au chiffrement faible, car ces clés ne sont pas aussi sécurisées que celles dont la taille est plus élevée.

Procédure

Étape 1 Accédez à **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificate (Certificat d'identité)** ou **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **Identity Certificate (Certificat d'identité)** ou **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **Code Signer (Signataire du code)**.

Étape 2 Pour autoriser des tailles de clés inférieures à 2 048 bits et des algorithmes de signature SHA-1, sous **Weak Crypto Configurations** (Configurations de chiffrement faible), cochez la case **Allow Weak Key Sizes and Hash Algorithms** (Autoriser des tailles de clé faible et des algorithmes de hachage).

Certificat de signataire de code

Importer un certificat de signataire de code

Pour importer un certificat de signataire de code, procédez comme suit :

Procédure

Étape 1 Dans le volet **Code Signer** (Signataire du code), cliquez sur **Import** (Importer) pour afficher la boîte de dialogue **Import Certificate** (Importer le certificat).

Étape 2 Entrez la phrase secrète utilisée pour déchiffrer le fichier au format PKCS12.

Étape 3 Saisissez le nom du fichier à importer ou cliquez sur **Browse** (Parcourir) pour afficher la boîte de dialogue **Import ID Certificate File** (Importer le fichier de certificat d'ID) et rechercher le fichier.

Étape 4 Sélectionnez le fichier à importer et cliquez sur **Import ID Certificate File** (Importer le fichier de certificat d'ID).

Le fichier de certificat sélectionné apparaît dans la boîte de dialogue **Import Certificate** (Importer le certificat).

Étape 5 Cliquez sur **Import Certificate** (Importer le certificat).

Le certificat importé apparaît dans le volet **Code Signer** (Signataire du code).

Étape 6 Cliquez sur **Apply** (Appliquer) pour enregistrer la configuration du certificat de signataire de code nouvellement importée.

Exporter un certificat de signataire de code

Pour exporter un certificat de signataire de code, procédez comme suit :

Procédure

Étape 1 Dans le volet **Code Signer** (Signataire du code), cliquez sur **Export** (Exporter) pour afficher la boîte de dialogue **Export Certificate** (Exporter le certificat).

Étape 2 Saisissez le nom du fichier de format PKCS12 à utiliser pour exporter la configuration du certificat.

Étape 3 Dans la zone **Certificate Format** (Format de certificat), pour utiliser la norme de cryptographie à clé publique, qui peut être codée en base64 ou au format hexadécimal, cliquez sur le bouton radio **PKCS12 format** (Format PKCS12). Sinon, cliquez sur le bouton radio **PEM format** (Format PEM).

Étape 4 Cliquez sur **Browse** (Parcourir) pour afficher la boîte de dialogue **Export ID Certificate File** (Exporter le fichier de certificat d'ID) pour trouver le fichier vers lequel vous souhaitez exporter la configuration du certificat.

Étape 5 Sélectionnez le fichier et cliquez sur **Export ID Certificate File** (Exporter le fichier de certificat d'ID).

Le fichier de certificat sélectionné apparaît dans la boîte de dialogue **Export Certificate** (Exporter le certificat).

Étape 6 Saisissez la phrase secrète utilisée pour déchiffrer le fichier au format PKCS12 pour l'exportation.

Étape 7 Confirmez la phrase secrète de déchiffrement.

Étape 8 Cliquez sur **Export Certificate** (Exporter le certificat) pour exporter la configuration du certificat.

Définir une alerte d'expiration de certificat (pour les certificats d'identité ou CA)

L'ASA vérifie tous les certificats CA et d'ID des points de confiance pour déterminer leur expiration une fois toutes les 24 heures. Si un certificat est sur le point d'expirer, un journal système sera émis en tant qu'alerte.

En plus du rappel de réabonnement, si un certificat déjà expiré est détecté dans la configuration, un journal système est généré une fois par jour pour rectifier la configuration en renouvelant le certificat ou en supprimant le certificat expiré.

Par exemple, supposons que les alertes d'expiration sont configurées pour commencer à 60 jours et se répètent ensuite tous les 6 jours. Si l'ASA est redémarré au bout de 40 jours, une alerte est envoyée ce jour-là et l'alerte suivante est envoyée le 36e jour.

Remarque La vérification de l'expiration n'est pas effectuée sur les certificats de groupe de confiance. Le point de confiance CA local est également traité comme un point de confiance normal pour la vérification de l'expiration.

Procédure

Étape 1 Accédez à **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificate/CA Certificate (Certificat d'identité/Certificat CA)**.

Étape 2 Cochez la case **Enable Certificate Expiration Alert** (Activer l'alerte d'expiration du certificat).

Étape 3 Indiquez le nombre de jours souhaité :

- Envoyer la première alerte avant : configurez le nombre de jours (de 1 à 90) avant l'expiration auxquels la première alerte sera émise.
- Répéter l'alerte pour : configurez la fréquence d'alerte (1 à 14 jours) si le certificat n'est pas renouvelé. Par défaut, la première alerte est envoyée 60 jours avant l'expiration et une fois par semaine après, jusqu'à ce que le certificat soit renouvelé et supprimé. De plus, une alerte est envoyée le jour de l'expiration, puis une fois par jour par la suite, et quelle que soit la configuration de l'alerte, une alerte est envoyée chaque jour pendant la dernière semaine précédant l'expiration.

Supervision des certificats numériques

Consultez les commandes suivantes pour superviser l'état du certificat numérique :

- **Monitoring (Supervision) > Properties (Propriétés) > CRL**

  Ce volet affiche les détails de la CRL.

- **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

Historique de gestion des certificats

Tableau 34 : Historique de gestion des certificats

Nom de la caractéristique	Versions de plateforme	Description
Certificate Management	7.0(1)	Les certificats numériques (y compris les certificats CA, les certificats d'identité et les certificats de signataire de code) fournissent une identification numérique pour l'authentification. Un certificat numérique contient des renseignements permettant d'identifier un appareil ou un utilisateur, tels que le nom, le numéro de série, l'entreprise, le service ou l'adresse IP. Les autorités de certification sont des autorités de confiance qui « signent » des certificats pour vérifier leur authenticité, garantissant ainsi l'identité du périphérique ou de l'utilisateur. Les autorités de certification émettent des certificats numériques dans le contexte d'une PKI, qui utilise le chiffrement par clé publique ou par clé privée pour assurer la sécurité. Nous avons introduit les écrans suivants : Configuration > Remote Access VPN (VPN d'accès à distance) > Certificate Management Configuration (Configuration de la gestion des certificats) > Site-to-Site VPN (VPN de site à site) > Certificate Management (Gestion des certificats). Nous avons introduit ou modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Certificate Management (Gestion des certificats) > CA Certificates Configuration (Configuration des certificats CA) > Device Management (Gestion des périphériques) > Certificate Management (Gestion des certificats) > CA Certificates (Certificats CA).
Certificate Management	7.2(1)	
Certificate Management	8.0(2)	

Nom de la caractéristique	Versions de plateforme	Description
Mandataire SCEP	v 8.4(1)	Nous avons introduit cette fonctionnalité, qui permet un déploiement sécurisé des certificats de périphérique à partir d'autorités de certification tierces.
Identités de référence	9.6(2)	Le traitement du client TLS prend désormais en charge les règles de vérification de l'identité de serveur définies dans la RFC 6125, section 6. La vérification de l'identité sera effectuée pendant la validation PKI pour les connexions TLS au serveur de journal système et au serveur de licences Smart uniquement. Si l'identité présentée ne correspond pas à l'identité de référence configurée, la connexion n'est pas établie. Nous avons modifié les écrans suivants : Configuration > Remote Access VPN (VPN d'accès à distance) > Advanced Configuration (Configuration avancée) > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Servers (Serveurs de journal système) > Add/Edit Configuration (Ajouter/Modifier la configuration) > Device Management (Gestion des périphériques) > Smart Call Home
Serveur CA local	9.12(1)	Pour que le FQDN de l'URL d'inscription soit configurable au lieu d'utiliser le FQDN configuré de l'ASA, une nouvelle option d'interface de ligne de commande est introduite. Cette nouvelle option est ajoutée au mode smpt du serveur CA de chiffrement. Nous avons rendu obsolète le serveur CA local et le supprimerons dans une version ultérieure : lorsque l'ASA est configuré en tant que serveur CA local, il est en mesure d'émettre des certificats numériques, de publier des listes de révocation de certificats (CRL) et de révoquer en toute sécurité les certificats émis. Cette fonctionnalité a été abandonnée et, par conséquent, la commande du serveur CA de chiffrement l'a été aussi.
Serveur CA local	9.13(1)	Nous avons supprimé la prise en charge du serveur CA local. Ainsi, la commande **crypto ca server** et ses sous-commandes sont supprimées. Nous avons supprimé les commandes suivantes : **crypto ca server** et toutes ses sous-commandes.
Modifications des commandes du point de distribution de la CRL	9.13(1)	Les commandes de configuration d'URL de CDP statiques sont supprimées et déplacées vers la commande de certificat correspondante. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)**

Nom de la caractéristique	Versions de plateforme	Description
Taille du cache de la CRL augmentée	9.13(1)	Pour éviter l'échec de téléchargements de CRL volumineux, la taille du cache a été augmentée et la limite du nombre d'entrées dans une CRL individuelle a été supprimée. • Augmentation de la taille totale du cache de la CRL à 16 Mo par contexte pour le mode de contexte multiple. • Augmentation de la taille totale du cache de la CRL à 128 Mo pour le mode de contexte unique.
Option de restauration des contrôles de validité du certificat de contournement	9.15(1)	L'option de contournement de la vérification de la révocation en raison de problèmes de connectivité avec le serveur CRL ou OCSP, qui avait été supprimée dans la version 9.13(1), a été rétablie.
Modifications apportées aux commandes de certificat correspondantes pour prendre en charge l'URL du point de distribution de la CRL statique	9.15(1)	La commande de configuration d'URL de CDP statiques a permis aux CDP statiques d'être mappés de façon unique à chaque certificat d'une chaîne validée. Cependant, un seul de ces mappages était pris en charge pour chaque certificat. Cette modification permet aux CDP configurés de manière statique d'être mappés à une chaîne de certificats pour l'authentification.
Les modifications apportées à la paire de clés du point de confiance et à la clé de chiffrement génèrent des commandes	9.16(1)	La prise en charge des certificats avec des tailles de clé inférieures à 2 048 a été supprimée. Toute configuration utilisant des options de 512, 768 ou 1 024 bits est transférée vers la version 2 048 avec notification dûe. La prise en charge de l'utilisation de l'algorithme de hachage SHA1 pour la certification a été supprimée. **Remarque** La commande **crypto ca permit-weak-crypto** a été introduite pour remplacer ces restrictions. La nouvelle option de clé EDDSA a été ajoutée aux options RSA et ECDSA existantes.



CHAPITRE 27

Inspection ARP et table des adresses MAC

Ce chapitre décrit comment personnaliser la table des adresses MAC et configurer l'inspection ARP pour les groupes de ponts.

- À propos de l'inspection ARP et de la table des adresses MAC, à la page 835
- Paramètres d'usine, à la page 836
- Lignes directrices pour l'inspection ARP et la table d'adresses MAC, à la page 837
- Configurer l'inspection ARP et les autres paramètres ARP, à la page 837
- Personnaliser la table des adresses MAC pour les groupes de ponts, à la page 839
- Historique de l'inspection ARP et de la table des adresses MAC, à la page 841

À propos de l'inspection ARP et de la table des adresses MAC

Pour les interfaces d'un groupe de ponts, l'inspection ARP empêche une attaque « man-in-the-middle ». Vous pouvez également personnaliser d'autres paramètres ARP. Vous pouvez personnaliser le tableau d'adresses MAC pour les groupes de ponts, y compris en ajoutant une entrée ARP statique pour éviter l'usurpation d'adresse MAC.

Inspection ARP pour le trafic de groupe de ponts

Par défaut, tous les paquets ARP sont autorisés entre les membres du groupe de ponts. Vous pouvez contrôler le flux de paquets ARP en activant l'inspection ARP.

L'inspection ARP empêche les utilisateurs malveillants d'usurper l'identité d'autres hôtes ou routeurs (connue sous le nom d'usurpation d'identité ARP). L'usurpation d'identité ARP peut permettre une attaque de l'intercepteur. Par exemple, un hôte envoie une requête ARP au routeur de passerelle; le routeur de passerelle répond par l'adresse MAC du routeur de passerelle. Cependant, l'agresseur envoie une autre réponse ARP à l'hôte avec l'adresse MAC de l'agresseur au lieu de l'adresse MAC du routeur. L'agresseur peut désormais intercepter tout le trafic de l'hôte avant de le transférer au routeur.

L'inspection ARP garantit qu'un agresseur ne peut pas envoyer une réponse ARP avec l'adresse MAC de l'agresseur, tant que la bonne adresse MAC et l'adresse IP associée figurent dans le tableau ARP statique.

Lorsque vous activez l'inspection ARP, ASA compare l'adresse MAC, l'adresse IP et l'interface source de tous les paquets ARP aux entrées statiques du tableau ARP, et effectue les actions suivantes :

- Si l'adresse IP, l'adresse MAC et l'interface source correspondent à une entrée ARP, le paquet est transmis.

- En cas de non-concordance entre l'adresse MAC, l'adresse IP ou l'interface, ASA abandonne le paquet.
- Si le paquet ARP ne correspond à aucune entrée dans le tableau ARP statique, vous pouvez définir ASA pour transférer le paquet hors de toutes les interfaces (flood) (submersion), ou pour abandonner le paquet.



Remarque L'interface dédiée Management (gestion) ne submerge jamais de paquets, même si ce paramètre est réglé à flood.

Tableau d'adresses MAC

Lorsque vous utilisez des groupes de ponts, l'ASA apprend et construit un tableau d'adresses MAC de la même manière qu'un pont ou un commutateur normal : lorsqu'un périphérique envoie un paquet par l'intermédiaire du groupe de ponts, l'ASA ajoute l'adresse MAC à son tableau. Le tableau associe l'adresse MAC à l'interface source de sorte que l'ASA sache envoyer tous les paquets adressés au périphérique par la bonne interface. Comme le trafic entre les membres du groupe de ponts est soumis à la politique de sécurité ASA, si l'adresse MAC de destination d'un paquet ne figure pas dans le tableau, l'ASA ne submerge pas le paquet d'origine sur toutes les interfaces comme un pont normal le fait. Au lieu de cela, il génère les paquets suivants pour les périphériques connectés directement ou pour les périphériques distants :

- Paquets pour les périphériques connectés directement : l'ASA génère une requête ARP pour l'adresse IP de destination, afin de pouvoir apprendre quelle interface reçoit la réponse ARP.
- Paquets pour les périphériques distants : l'ASA génère un message ping vers l'adresse IP de destination afin de pouvoir apprendre quelle interface reçoit la réponse ping.

Le paquet d'origine est abandonné.

Pour le mode routé, vous pouvez éventuellement activer la submersion des paquets non IP sur toutes les interfaces.

Paramètres d'usine

- Si vous activez l'inspection ARP, le paramètre par défaut est d'inonder les paquets non correspondants.
- La valeur du délai d'expiration par défaut pour les entrées du tableau d'adresses MAC dynamiques est de 5 minutes.
- Par défaut, chaque interface apprend automatiquement les adresses MAC du trafic d'entrée et ASA ajoute les entrées correspondantes au tableau d'adresses MAC.



Remarque Cisco Secure Firewall ASA génère un paquet de réinitialisation pour réinitialiser une connexion qui est refusée par un moteur d'inspection dynamique. Ici, l'adresse MAC de destination du paquet n'est pas déterminée en fonction de la recherche de la table ARP, mais est plutôt tirée directement des paquets (connexions) qui sont refusés.

Lignes directrices pour l'inspection ARP et la table d'adresses MAC

- L'inspection ARP n'est possible que pour les groupes de ponts.
- La configuration de la table des adresses MAC n'est possible que pour les groupes de ponts.

Configurer l'inspection ARP et les autres paramètres ARP

Pour les groupes de ponts, vous pouvez activer l'inspection ARP. Vous pouvez également configurer d'autres paramètres ARP pour les groupes de ponts et pour les interfaces en mode routé.

Procédure

Étape 1 Ajoutez des entrées ARP statiques en fonction de Ajouter une entrée ARP statique et personnaliser d'autres paramètres ARP, à la page 837. L'inspection ARP compare les paquets ARP avec les entrées ARP statiques dans le tableau ARP. Par conséquent, des entrées ARP statiques sont nécessaires pour cette fonctionnalité. Vous pouvez également configurer d'autres paramètres ARP.

Étape 2 Activez l'inspection ARP conformément à Activer l'inspection ARP, à la page 838.

Ajouter une entrée ARP statique et personnaliser d'autres paramètres ARP

Par défaut, pour les groupes de ponts, tous les paquets ARP sont autorisés entre les interfaces membres des groupes de ponts. Vous pouvez contrôler le flux de paquets ARP en activant l'inspection ARP. L'inspection ARP compare les paquets ARP avec les entrées ARP *statiques* dans le tableau ARP.

Pour les interfaces routées, vous pouvez saisir des entrées ARP statiques, mais normalement, les entrées dynamiques sont suffisantes. Pour les interfaces routées, la table ARP est utilisée pour acheminer des paquets aux hôtes connectés directement. Bien que les expéditeurs identifient la destination d'un paquet par une adresse IP, la livraison réelle du paquet sur Ethernet dépend de l'adresse MAC Ethernet. Lorsqu'un routeur ou un hôte souhaite acheminer un paquet sur un réseau directement connecté, il envoie une requête ARP demandant l'adresse MAC associée à l'adresse IP, puis achemine le paquet à l'adresse MAC en fonction de la réponse ARP. L'hôte ou le routeur conserve une table ARP pour ne pas avoir à envoyer des demandes ARP pour chaque paquet à livrer. La table ARP est mise à jour dynamiquement chaque fois que des réponses ARP sont envoyées sur le réseau et, si une entrée n'est pas utilisée pendant un certain temps, elle expire. Si une entrée est incorrecte (par exemple, l'adresse MAC change pour une adresse IP donnée), l'entrée doit expirer avant de pouvoir être mise à jour avec les nouvelles informations.

En mode transparent, l'ASA utilise uniquement les entrées ARP dynamiques de la table ARP pour le trafic entrant et sortant de l'ASA, tel que le trafic de gestion.

Vous pouvez également définir le délai d'expiration d'ARP et d'autres comportements d'ARP.

Procédure

Étape 1 Choisissez **Configuration** > **Gestion des périphériques** > **Avancé** > **ARP** > **Tableau statique ARP**.

Étape 2 Cliquez sur **Ajouter** pour ajouter une entrée ARP statique.

La boîte de dialogue**Add ARP Static Configuration** (Ajouter une configuration ARP statique) apparaît.

a) Choisissez l'interface connectée au réseau hôte dans la liste déroulante **Interface**.
b) Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de l'hôte.
c) Saisissez l'adresse MAC de l'hôte dans le champ **MAC Address** (adresse MAC); par exemple, 00e0.1e4e.3d8b.
d) Cochez la case **Proxy ARP** (Serveur mandataire ARP) pour effectuer un mandataire ARP pour cette adresse.

Si l'ASA reçoit une requête ARP pour l'adresse IP précisée, il répond avec l'adresse MAC précisée.

e) Cliquez sur **OK**.

Étape 3 Saisissez une valeur dans le champ Délai d'expiration **ARP** afin de définir le délai d'expiration ARP pour les entrées ARP *dynamiques*.

Ce champ définit le délai avant que l'ASA recrée la table ARP, entre 60 et 4294967 secondes. La valeur par défaut est de 14400 secondes. La reconstitution de la table ARP met automatiquement à jour les nouvelles informations sur l'hôte et supprime les anciennes. Vous pourriez souhaiter réduire le délai d'expiration, car les informations sur l'hôte changent fréquemment.

Étape 4 Pour autoriser les sous-réseaux non connectés, cochez la case **Allow non-connected subnets** (autoriser les sous-réseaux non connectés). Le cache ARP de l'ASA contient uniquement les entrées des sous-réseaux connectés directement par défaut. Vous pouvez activer le cache ARP pour inclure également les sous-réseaux non connectés directement. Nous vous déconseillons d'activer cette fonctionnalité, sauf si vous connaissez les risques de sécurité. Cette fonctionnalité pourrait faciliter les attaques par déni de service contre l'ASA; un utilisateur, sur n'importe quelle interface, pourrait envoyer de nombreuses réponses ARP et sur téléverser la table ARP de l'ASA de fausses entrées.

Vous souhaiterez peut-être utiliser cette fonctionnalité si vous utilisez :

- Sous-réseaux secondaires.
- Serveur mandataire ARP sur les routes adjacentes pour le transfert du trafic.

Étape 5 Saisissez une valeur dans le champ **Rate-Limit ARP** (Limite de débit ARP) pour contrôler le nombre de paquets ARP par seconde sur toutes les interfaces.

Saisissez une valeur entre 10 et 32 768. La valeur par défaut dépend de votre modèle d'ASA. Vous pouvez personnaliser cette valeur pour empêcher une attaque de tempête ARP.

Étape 6 Cliquez sur **Apply** (Appliquer).

Activer l'inspection ARP

Cette section décrit comment activer l'inspection ARP pour les groupes de ponts.

Procédure

Étape 1 Choisissez le volet **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **ARP** > **ARP Inspection (Inspection ARP)**.

Étape 2 Choisissez la ligne d'interface sur laquelle vous souhaitez activer l'inspection ARP, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Edit ARP Inspection (Modifier l'inspection ARP) apparaît.

Étape 3 Cochez la case **Enable ARP Inspection** (Activer l'inspection ARP) pour activer l'inspection ARP.

Étape 4 (Facultatif) Cochez la case **Flood ARP Packets** (Inonder les paquets ARP) pour inonder les paquets ARP non correspondants.

Par défaut, les paquets qui ne correspondent à aucun élément d'une entrée ARP statique sont inondés sur toutes les interfaces, à l'exception de l'interface d'origine. En cas de non-concordance entre l'adresse MAC, l'adresse IP ou l'interface, l'ASA abandonne le paquet.

Si vous décochez cette case, tous les paquets non correspondants sont abandonnés, ce qui limite le protocole ARP par l'ASA aux entrées statiques.

Remarque L'interface Management 0/0 ou 0/1 ou la sous-interface, si elle est présente, ne submerge jamais de paquets, même si ce paramètre est réglé sur flood.

Étape 5 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Personnaliser la table des adresses MAC pour les groupes de ponts

Cette section décrit comment vous pouvez personnaliser le tableau d'adresses MAC pour les groupes de ponts.

Ajouter une adresse MAC statique pour les groupes de ponts

Normalement, les adresses MAC sont ajoutées au tableau d'adresses MAC de manière dynamique au fur et à mesure que le trafic en provenance d'une adresse MAC particulière entre dans une interface. Vous pouvez ajouter des adresses MAC statiques au tableau d'adresses MAC. L'ajout d'entrées statiques offre l'avantage de prévenir l'usurpation d'adresse MAC. Si un client avec la même adresse MAC qu'une entrée statique tente d'envoyer le trafic vers une interface qui ne correspond pas à l'entrée statique, l'ASA abandonne le trafic et génère un message système. Lorsque vous ajoutez une entrée ARP statique (voir Ajouter une entrée ARP statique et personnaliser d'autres paramètres ARP, à la page 837), une entrée d'adresse MAC statique est automatiquement ajoutée au tableau d'adresses MAC.

Pour ajouter une adresse MAC statique au tableau d'adresses MAC, procédez comme suit.

Procédure

Étape 1 Choisissez le volet **Configuration** > **Device Setup** > **Bridging** > **MAC Address Table** (tableau d'adresses MAC de configuration du périphérique).

Étape 2 (Facultatif) Saisissez une valeur dans le champ Dynamic entry Timeout (délai d'expiration de l'entrée dynamique) pour définir la durée pendant laquelle une entrée d'adresse MAC reste dans le tableau d'adresses MAC avant d'expirer.

Cette valeur est comprise entre 5 et 720 minutes (12 heures). La valeur par défaut est de 5 minutes.

Étape 3 Cliquez sur **Add (Ajouter)**.

La boîte de dialogue Add MAC Address entry (ajouter une entrée d'adresse MAC) s'affiche.

Étape 4 Choisissez l'interface source associée à l'adresse MAC dans la liste déroulante Interface Name (nom de l'interface).

Étape 5 Saisissez l'adresse MAC dans le champ MAC Address (adresse MAC).

Étape 6 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Configurer l'apprentissage de l'adresse MAC

Par défaut, chaque interface apprend automatiquement les adresses MAC du trafic d'entrée et l'ASA ajoute les entrées correspondantes au tableau d'adresses MAC. Vous pouvez désactiver l'apprentissage des adresses MAC si vous le souhaitez; cependant, à moins que vous ajoutiez statiquement des adresses MAC au tableau, aucun trafic ne peut passer par l'ASA. En mode routé, vous pouvez activer la submersion des paquets non IP sur toutes les interfaces.

Pour configurer l'apprentissage des adresses MAC, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **Bridging (Pontage)** > **MAC Learning (Apprentissage MAC)** .

Étape 2 Pour désactiver l'apprentissage MAC, choisissez une ligne d'interface et cliquez sur **Disable** (Désactiver).

Étape 3 Pour réactiver l'apprentissage MAC, cliquez sur **Enable** (Activer).

Étape 4 Pour activer la submersion de paquets non IP, cochez la case **Enable flooding for unknown MAC address for non IPv4-IPv6 packets** (Activer l'inondation en adresse MAC inconnue pour les paquets non IPv4-IPv6).

Étape 5 Cliquez sur **Apply** (Appliquer).

Historique de l'inspection ARP et de la table des adresses MAC

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Inspection ARP	7.0(1)	L'inspection ARP compare l'adresse MAC, l'adresse IP et l'interface source de tous les paquets ARP aux entrées statiques du tableau ARP. Cette fonctionnalité est disponible pour le mode de pare-feu transparent et pour les interfaces d'un groupe de ponts en mode transparent et en mode routé à partir de la version 9.7(1). Nous avons introduit les commandes suivantes : **arp**, **arp-inspection** et **show arp-inspection**.
Tableau d'adresses MAC	7.0(1)	Vous souhaiterez peut-être personnaliser le tableau des adresses MAC pour le mode transparent et pour les interfaces d'un groupe de ponts en mode transparent et en mode routé à partir de la version 9.7(1). Nous avons introduit les commandes suivantes : **mac-address-table static**, **mac-address-table aging-time**, **mac-learn disable** et **show mac-address-table**.
Ajouts de cache ARP pour les sous-réseaux non connectés	8.4(5)/9.1(2)	Le cache ARP de l'ASA contient uniquement les entrées des sous-réseaux connectés directement par défaut. Vous pouvez désormais activer le cache ARP pour inclure également les sous-réseaux non connectés directement. Nous vous déconseillons d'activer cette fonctionnalité, sauf si vous connaissez les risques de sécurité. Cette fonctionnalité pourrait faciliter les attaques par déni de service contre l'ASA; un utilisateur, sur n'importe quelle interface, pourrait envoyer de nombreuses réponses ARP et sur téléverser la table ARP de l'ASA de fausses entrées. Vous souhaiterez peut-être utiliser cette fonctionnalité si vous utilisez : • Sous-réseaux secondaires. • Serveur mandataire ARP sur les routes adjacentes pour le transfert du trafic. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > ARP > ARP Static Table (Tableau statique ARP).

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Limitation de débit ARP personnalisable	9.6(2)	Vous pouvez définir le nombre maximum de paquets ARP autorisés par seconde. La valeur par défaut dépend de votre modèle d'ASA. Vous pouvez personnaliser cette valeur pour empêcher une attaque de tempête ARP. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **ARP** > **ARP Static Table (Tableau statique ARP)**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage et pont intégrés	9.7(1)	Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que l'ASA relie par des ponts au lieu de routes. L'ASA n'est pas un vrai pont, car l'ASA continue d'agir comme un pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place. Auparavant, vous ne pouviez configurer les groupes de ponts qu'en mode de pare-feu transparent, où vous ne pouvez pas effectuer d'acheminement entre les groupes de ponts. Cette fonctionnalité vous permet de configurer des groupes de ponts en mode de pare-feu routé et pour effectuer le routage entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une solution de rechange au commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur l'ASA à affecter au groupe de ponts. En mode routé, les BVI peuvent être une interface nommée et participer séparément des interfaces membres à certaines fonctionnalités, telles que les règles d'accès et le serveur DHCP. Les fonctionnalités suivantes, prises en charge en mode transparent, ne sont pas prises en charge en mode routé : mode de contexte multiple, mise en grappe d'ASA. Les fonctionnalités suivantes ne sont pas prises en charge sur les BVI : le routage dynamique et le routage de multidiffusion. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Static Routes (Routes statiques)** **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Server (Serveur DHCP)** **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Critères d'accès)** **Configuration** > **Firewall (Pare-feu)** > **EtherType Rules (Règles EtherType)**



PARTIE V

Routage IP

- Aperçu du routage, à la page 847
- Routages statiques et par défaut, à la page 863
- Routage basé sur une stratégie, à la page 873
- Cartes de routage, à la page 883
- Routage par détection de transfert bidirectionnel (BFD), à la page 893
- BGP, à la page 901
- OSPF, à la page 931
- IS-IS, à la page 987
- EIGRP, à la page 1015
- Routage multidiffusion, à la page 1037



CHAPITRE 28

Aperçu du routage

Ce chapitre décrit le comportement du routage dans l'ASA.

- Détermination du chemin, à la page 847
- Types de routage pris en charge, à la page 848
- Protocoles Internet pris en charge pour le routage, à la page 849
- Table de routage, à la page 850
- Table de routage pour le trafic de gestion, à la page 858
- Routage à chemins multiples à coûts égaux (ECMP), à la page 859
- Désactiver les demandes ARP du mandataire, à la page 860
- Afficher la table de routage, à la page 861
- Historique de l'aperçu du routage, à la page 861

Détermination du chemin

Les protocoles de routage utilisent des métriques pour évaluer quel chemin sera le meilleur à parcourir pour un paquet. Une métrique est une norme de mesure, telle que la bande passante du chemin, utilisée par les algorithmes de routage pour déterminer le chemin optimale vers une destination. Pour faciliter le processus de détermination du chemin, les algorithmes de routage lancent et gèrent les tableaux de routage, qui comprennent les informations de routage. Les informations de route varient en fonction de l'algorithme de routage utilisé.

Les algorithmes de routage remplissent les tableaux de routage avec diverses informations. Les associations de destination ou du prochain saut indiquent à un routeur qu'une destination particulière peut être atteinte de manière optimale en envoyant le paquet à un routeur particulier représentant le prochain saut sur le chemin vers la destination finale. Lorsqu'un routeur reçoit un paquet entrant, il vérifie l'adresse de destination et tente d'associer cette adresse à un saut suivant.

Les tableaux de routage peuvent également comprendre d'autres informations, telles que des données sur l'opportunité d'un chemin. Les routeurs comparent les métriques pour déterminer les routes optimales. Ces métriques varient en fonction de la conception de l'algorithme de routage utilisé.

Les routeurs communiquent entre eux et gèrent leurs tables de routage par la transmission de divers messages. Le message de mise à jour du routage en est un qui consiste généralement en tout ou en partie d'une table de routage. En analysant les mises à jour de routage de tous les autres routeurs, votre routeur peut dresser un tableau détaillé de la topologie du réseau. Une annonce d'état de lien, un autre exemple de message envoyé entre des routeurs, informe les autres routeurs de l'état des liens de l'expéditeur. Les informations sur la liaison

peuvent également être utilisées pour dresser une image complète de la topologie du réseau afin de permettre aux routeurs de déterminer les routes optimales vers les destinations du réseau.

Remarque Le routage symétrique est uniquement pris en charge pour le basculement actif/actif dans le mode de contexte multiple.

Types de routage pris en charge

Un routeur peut utiliser plusieurs types de routage. L'ASA utilise les types de routage suivants :

- Statique ou dynamique
- Chemin unique ou chemin multiple
- Non hiérarchique ou hiérarchique
- État de lien ou vecteur de distance

Statique ou dynamique

Les algorithmes de routage statique sont en fait des mappages de tables établis par l'administrateur réseau. Ces mappages ne changent pas, sauf si l'administrateur réseau les modifie. Les algorithmes qui utilisent des routes statiques sont simples à concevoir et fonctionnent bien dans des environnements où le trafic réseau est relativement fiable et où la conception de réseau est relativement simple.

Étant donné que les systèmes de routage statique ne peuvent pas réagir aux modifications du réseau, ils sont généralement considérés comme ne convenant pas aux grands réseaux en constante évolution. La plupart des algorithmes de routage prédominants sont des algorithmes de routage dynamique, qui s'adaptent aux circonstances changeantes du réseau en analysant les messages de mise à jour de routage entrants. Si le message indique qu'un changement de réseau est survenu, le logiciel de routage recalcule les routages et envoie de nouveaux messages de mise à jour de routage. Ces messages pénètrent dans le réseau, incitant les routeurs à réexécuter leurs algorithmes et à modifier leurs tables de routage en conséquence.

Les algorithmes de routage dynamique peuvent être complétés par des routes statiques, le cas échéant. Un routeur de dernier recours (une voie de routage par défaut pour un routeur auquel tous les paquets non routables sont envoyés), par exemple, peut être désigné pour servir de référentiel pour tous les paquets non routables, garantissant que tous les messages sont au moins gérés d'une manière ou d'une autre.

Chemin unique ou chemin multiple

Certains protocoles de routage sophistiqués prennent en charge plusieurs chemins vers la même destination. Contrairement aux algorithmes à chemin unique, ces algorithmes à chemins multiples permettent le multiplexage du trafic sur plusieurs lignes. Les avantages des algorithmes par chemins multiples sont un débit et une fiabilité considérablement meilleurs, ce qui est généralement appelé partage de charge.

Non hiérarchique ou hiérarchique

Certains algorithmes de routage fonctionnent dans un espace à plat, tandis que d'autres utilisent des hiérarchies de routage. Dans un système de routage à plat, les routeurs sont les homologues de tous les autres. Dans un système de routage hiérarchique, certains routeurs forment ce qui équivaut à un réseau fédérateur (backbone) de routage. Les paquets provenant de routeurs ne faisant pas partie du réseau fédérateur sont acheminés vers les routeurs de ce dernier, où ils sont envoyés à travers le réseau fédérateur jusqu'à ce qu'ils atteignent la zone générale de la destination. À ce stade, ils se déplacent du dernier routeur de réseau fédérateur à un ou plusieurs routeurs hors du réseau fédérateur jusqu'à la destination finale.

Les systèmes de routage désignent souvent des groupes logiques de nœuds, appelés domaines, systèmes autonomes ou zones. Dans les systèmes hiérarchiques, certains routeurs d'un domaine peuvent communiquer avec les routeurs d'autres domaines, tandis que d'autres ne peuvent communiquer qu'avec les routeurs de leur domaine. Dans les très grands réseaux, il peut exister des niveaux hiérarchiques supplémentaires, les routeurs du niveau hiérarchique le plus élevé constituant le réseau fédérateur de routage.

Le principal avantage du routage hiérarchique est qu'il imite l'organisation de la plupart des entreprises et, par conséquent, prend bien en charge leurs schémas de trafic. La plupart des communications réseau se produisent au sein de petits groupes d'entreprise (domaines). Comme les routeurs intra-domaines n'ont besoin de connaître que les autres routeurs de leur domaine, leurs algorithmes de routage peuvent être simplifiés et, selon l'algorithme de routage utilisé, le trafic de mise à jour de routage peut être réduit en conséquence.

État de lien ou vecteur de distance

Les algorithmes d'état de liens (également appelés algorithmes du plus court chemin d'abord) acheminent les informations de routage à tous les nœuds de l'inter-réseau. Cependant, chaque routeur envoie uniquement la partie de la table de routage qui décrit l'état de ses propres liaisons. Dans les algorithmes à état de liens, chaque routeur construit une image de l'ensemble du réseau dans ses tables de routage. Les algorithmes de vecteurs de distance (également appelés algorithmes de Bellman-Ford) exigent que chaque routeur envoie la totalité ou une partie de sa table de routage, mais uniquement à ses voisins. En gros, les algorithmes à état de liens envoient de petites mises à jour partout, tandis que les algorithmes à vecteur de distance envoient des mises à jour plus volumineuses uniquement aux routeurs voisins. Les algorithmes de vecteurs de distance ne connaissent que leurs voisins. En règle générale, les algorithmes d'état de liaison sont utilisés conjointement avec les protocoles de routage OSPF.

Protocoles Internet pris en charge pour le routage

L'ASA prend en charge plusieurs protocoles Internet pour le routage. Chaque protocole est décrit brièvement dans cette section.

- Protocole de routage de passerelle intérieure amélioré (EIGRP)

  EIGRP est un protocole exclusif de Cisco qui assure la compatibilité et une interopération transparente avec les routeurs IGRP. Un mécanisme de redistribution automatique permet aux routes IGRP d'être importées dans le protocole Enhanced IGRP, et inversement. Il est donc possible d'ajouter progressive-ment le protocole Enhanced IGRP à un réseau IGRP existant.

- Open Shortest Path First (OSPF)

  OSPF est un protocole de routage mis au point pour les réseaux IP (Internet Protocol) par le groupe de travail IGP (Interior Gateway Protocol) de l'Internet Engineering Task Force (IETF). OSPF utilise un algorithme d'état de liens pour créer et calculer le chemin le plus court vers toutes les destinations connues.

Chaque routeur d'une zone OSPF comprend une base de données d'états de liaison identique, qui est une liste de chacune des interfaces utilisables et des voisins accessibles du routeur.

- Protocole RIP (Routing Information Protocol)

  IPS est un protocole de vecteur de distance qui utilise le nombre de sauts comme mesure. Il s'agit d'un protocole IGP (Interior Gateway Protocol), ce qui signifie qu'il effectue le routage au sein d'un seul système autonome.

- Protocole de routage BGP

  BGP est un protocole de routage de système inter autonome. BGP est utilisé pour échanger des informations de routage pour Internet et est le protocole utilisé entre les fournisseurs de services Internet (ISP). Les clients se connectent aux fournisseurs de services Internet, et les fournisseurs de services Internet utilisent BGP pour échanger les routes du client et des fournisseurs de services Internet. Lorsque BGP est utilisé entre des systèmes autonomes (AS), le protocole est appelé BGP externe (EBGP). Si un fournisseur de services utilise BGP pour échanger des routages au sein d'un système autonome, le protocole est appelé BGP intérieur (IBGP).

- Intermediate System-to-Intermediate System (IS-IS)

  IS-IS est un protocole IGP (Interior Gateway Protocol) à état de liaison. Les protocoles à état de liaison se caractérisent par la propagation des informations nécessaires pour créer une carte complète de la connectivité du réseau sur chaque routeur participant. Cette carte est ensuite utilisée pour calculer le chemin le plus court vers les destinations.

Routage du trafic GRE

Dans ASA, le trafic d'encapsulation de routage générique (GRE) est géré à l'aide de flux bidirectionnels. Cela signifie que chaque session GRE est représentée par une seule entrée de flux qui gère le trafic entrant et sortant entre les points terminaux. Avec les flux bidirectionnels, une seule recherche de routage est effectuée et les deux directions sont mappées sur la même interface. Par conséquent, le système ne peut pas prendre de décisions de routage indépendantes pour chaque direction, ce qui peut entraîner un routage sous-optimal dans certains scénarios.

Table de routage

L'ASA utilise des tableaux de routage distincts pour le trafic de données (via le périphérique) et pour le trafic de gestion (du périphérique). Cette section décrit le fonctionnement des tables de routage. Pour en savoir plus sur la table de routage de gestion, consultez également Table de routage pour le trafic de gestion, à la page 858.

Mode de remplissage de la table de routage

La table de routage ASA peut être remplie par des routes définies de manière statique, des routes connectées directement et des routes découvertes par les protocoles de routage dynamique. Comme le périphérique ASA peut exécuter plusieurs protocoles de routage en plus d'avoir des routes statiques et connectées dans la table de routage, il est possible qu'une même route soit découverte ou saisie de plusieurs manières. Lorsque deux routes vers la même destination sont mises dans la table de routage, celle qui reste dans la table de routage est déterminée comme suit :

- Si les deux routes ont des longueurs de préfixe de réseau différentes (masques de réseau), les deux routes sont considérées comme uniques et sont entrées dans la table de routage. La logique de transfert de paquets détermine ensuite laquelle des deux utiliser.

  Par exemple, si les processus RIP et OSPF ont découvert les routes suivantes :

  - RIP : 192.168.32.0/24
  - OSPF : 192.168.32.0/19

  Même si les routes OSPF ont la meilleure distance administrative, les deux routes sont installées dans la table de routage, car chacune de ces routes a une longueur de préfixe différente (masque de sous-réseau). Ce sont des destinations considérées comme différentes et la logique de transfert de paquets détermine la route à utiliser.

- Si le périphérique ASA connaît plusieurs chemins vers la même destination à partir d'un protocole de routage unique, comme RIP, la voie de routage avec la meilleure mesure (déterminée par le protocole de routage) est entrée dans la table de routage.

  Les métriques sont des valeurs associées à des routes spécifiques, de la plus préférée à la moins préférée. Les paramètres utilisés pour déterminer les métriques varient selon le protocole de routage. Le chemin avec la mesure la plus basse est sélectionné comme chemin optimale et installé dans la table de routage. S'il existe plusieurs chemins vers la même destination avec des métriques égales, l'équilibrage de la charge est effectué sur ces chemins de coût égal.

- Si le périphérique ASA connaît une destination à partir de plus d'un protocole de routage, les distance administratives des routages sont comparées et les routes avec une distance administrative inférieure sont entrées dans la table de routage.

Distances administratives pour les routages

Vous pouvez modifier les distance administratives pour les routages détectés ou redistribués dans un protocole de routage. Si deux routes de deux protocoles de routage différents ont la même distance administrative, la route avec la distance administrative *par défaut* la plus faible est entrée dans la table de routage. Dans le cas des routes EIGRP et OSPF, si la route EIGRP et la route OSPF ont la même distance administrative, la route EIGRP est choisie par défaut.

La distance administrative est un paramètre de routage que ASA utilise pour sélectionner le meilleur chemin lorsqu'il existe deux ou plusieurs itinéraires différents vers la même destination à partir de deux protocoles de routage différents. Puisque les protocoles de routage ont des mesures basées sur des algorithmes différents des autres protocoles, il n'est pas toujours possible de déterminer le meilleur chemin pour deux routages vers la même destination qui ont été générées par différents protocoles de routage.

Chaque protocole de routage est priorisé à l'aide d'une valeur de distance administrative. Le tableau suivant présente les valeurs de distance administrative par défaut pour les protocoles de routage pris en charge par ASA.

Tableau 35 : Distance administrative par défaut pour les protocoles de routage pris en charge

Source de la route	Distance administrative par défaut
Interface connectée	0
Routage VPN	1

Source de la route	Distance administrative par défaut
Routage statique	1
Routage résumé EIGRP	5
BGP externe	20
EIGRP interne	90
OSPF	110
IS-IS	115
RIP	120
Routage EIGRP externe	170
BGP interne et local	200
Inconnu	255

Plus la valeur de la distance administrative est faible, plus la préférence est donnée au protocole. Par exemple, si l'ASA reçoit une voie de routage vers un certain réseau d'un processus de routage OSPF (distance administrative par défaut - 110) et d'un processus de routage RIP (distance administrative par défaut - 120), l'ASA choisit la voie de routage OSPF, car OSPF a une préférence plus élevée. Dans ce cas, le routeur ajoute la version OSPF de la route à la table de routage.

Une route VPN annoncée (V-Route/RRI) équivaut à une route statique avec la distance administrative par défaut de 1. Mais elle comporte une préférence plus élevée, comme avec le masque de réseau 255.255.255.255.

Dans cet exemple, si la source de routage dérivée OSPF était perdue (par exemple, en raison d'une coupure de courant), l'ASA utiliserait alors le routage dérivé RIP jusqu'à ce que le routage dérivé OSPF réapparaisse.

La distance administrative est un paramètre local. Par exemple, si vous modifiez la distance administrative des routages obtenus par OSPF, cette modification n'affectera que la table de routage de l'ASA pour lequel la commande a été saisie. La distance administrative n'est pas annoncée dans les mises à jour de routage.

La distance administrative n'affecte pas le processus de routage. Les processus de routage n'annoncent que les routages détectés par le processus de routage ou redistribués dans le processus de routage. Par exemple, le processus de routage RIP annonce les routes RIP, même si les routes découvertes par le processus de routage OSPF sont utilisées dans la table de routage.

Sauvegarde des routes dynamiques et statiques flottantes

Une route de secours est enregistrée lorsque la tentative initiale d'installation de la route dans la table de routage échoue parce qu'une autre route a été installée à la place. Si la voie de routage qui a été installée dans la table de routage échoue, le processus de maintenance de la table de routage appelle chaque processus de protocole de routage qui a enregistré une voie de routage de secours et lui demande de réinstaller la voie de routage dans la table de routage. S'il existe plusieurs protocoles avec des routes de secours enregistrées pour la voie de routage ayant échoué, la voie de routage préférée est choisie en fonction de la distance administrative.

Grâce à ce processus, vous pouvez créer des routes statiques flottantes qui sont installées dans la table de routage lorsque la route découverte par un protocole de routage dynamique échoue. Une voie de routage statique flottante est tout simplement une voie de routage statique configurée avec une distance administrative supérieure à celle des protocoles de routage dynamique s'exécutant sur ASA. Lorsque la voie de routage

correspondante découverte par un processus de routage dynamique échoue, la voie de routage statique est installée dans la table de routage.

Prise des décisions de transfert

Les décisions de transfert sont prises comme suit :

- Si la destination ne correspond à aucune entrée de la table de routage, le paquet est acheminé par l'intermédiaire de l'interface spécifiée pour la voie de routage par défaut. Si une voie de routage par défaut n'a pas été configurée, le paquet est rejeté.
- Si la destination correspond à une seule entrée dans la table de routage, le paquet est acheminé par l'interface associée à cette voie de routage.
- Si la destination correspond à plus d'une entrée dans la table de routage, le paquet est transféré hors de l'interface associée à la voie de routage qui a la plus grande longueur de préfixe de réseau.

Par exemple, un paquet destiné à 192.168.32.1 arrive sur une interface avec les routes suivantes dans la table de routage :

- Passerelle 192.168.32.0/24 10.1.1.2
- Passerelle 192.168.32.0/19 10.1.1.3

Dans ce cas, un paquet destiné à 192.168.32.1 est dirigé vers 10.1.1.2, car 192.168.32.1 fait partie du réseau 192.168.32.0/24. Il fait également partie de l'autre voie de routage dans la table de routage, mais 192.168.32.0/24 a le préfixe le plus long dans la table de routage (24 bits vers 19 bits). Les préfixes les plus longs sont toujours préférables aux plus courts lors du transfert d'un paquet.

Remarque Les connexions existantes continuent d'utiliser leurs interfaces établies même si une nouvelle connexion similaire entraînerait un comportement différent en raison d'une modification des routages.

Routage dynamique et Basculement

Les routages dynamiques sont synchronisés sur l'unité de secours lorsque la table de routage change sur l'unité active. Cela signifie que tous les ajouts, suppressions ou modifications effectués sur l'unité active sont immédiatement répercutés sur l'unité en veille. Si l'unité de secours devient active dans une paire actif/secours Basculement prête, elle aura déjà une table de routage identique à celle de l'unité active précédente, car les routages sont synchronisés dans le cadre de la synchronisation en bloc Basculement et des processus de duplication continue.

Routage et mise en grappe dynamiques

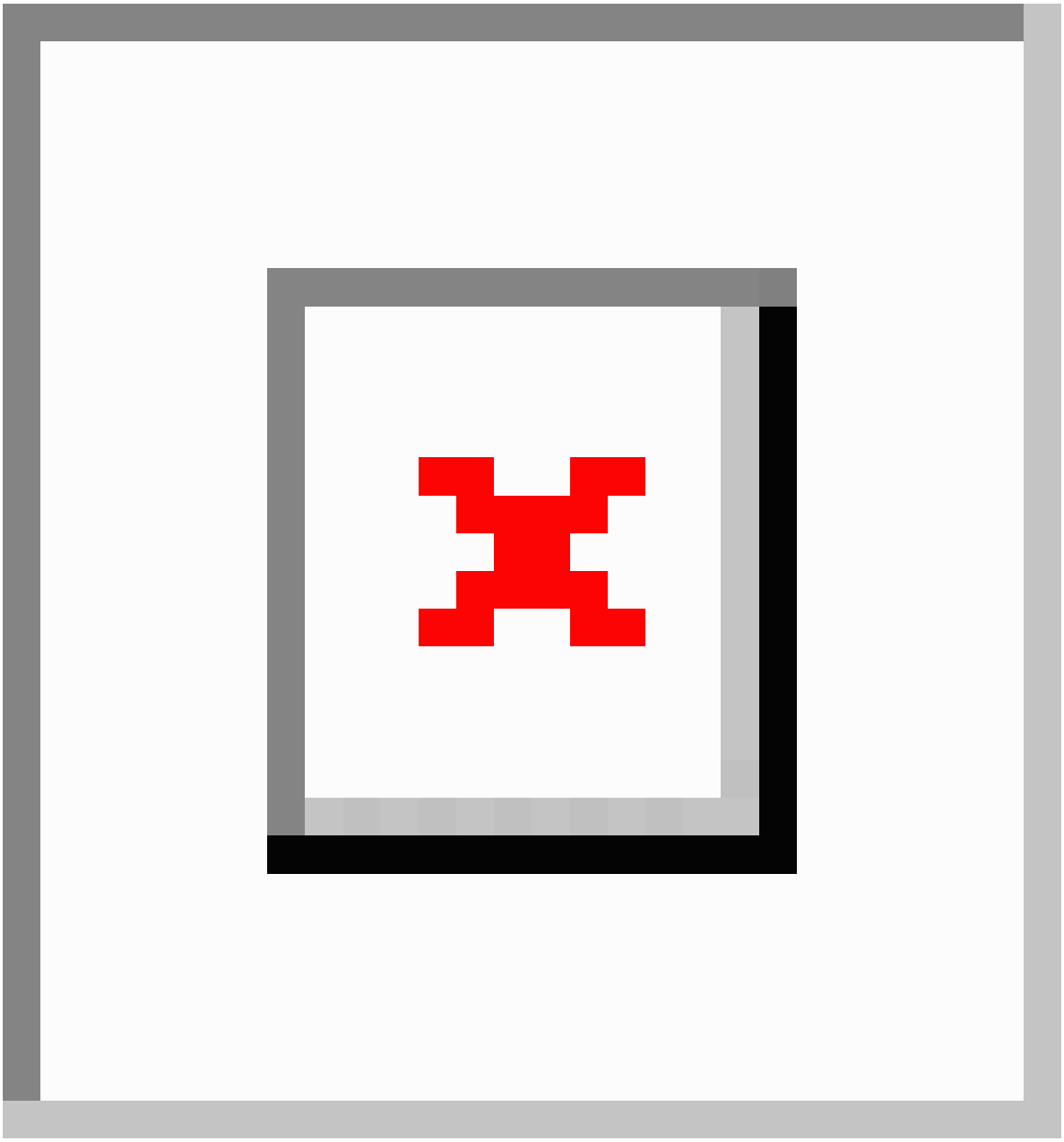
Cette section décrit comment utiliser le routage dynamique avec la mise en grappe.

Routage dynamique en mode EtherChannel étendu

Remarque IS-IS n’est pas pris en charge en mode EtherChannel étendu.

Le processus de routage ne s’exécute que sur le nœud de contrôle, et les routes sont apprises par le nœud de contrôle et répliquées sur les nœuds de données. Si un paquet de routage arrive à un nœud de données, il est redirigé vers le nœud de contrôle.

Illustration 80 : Routage dynamique en mode EtherChannel étendu



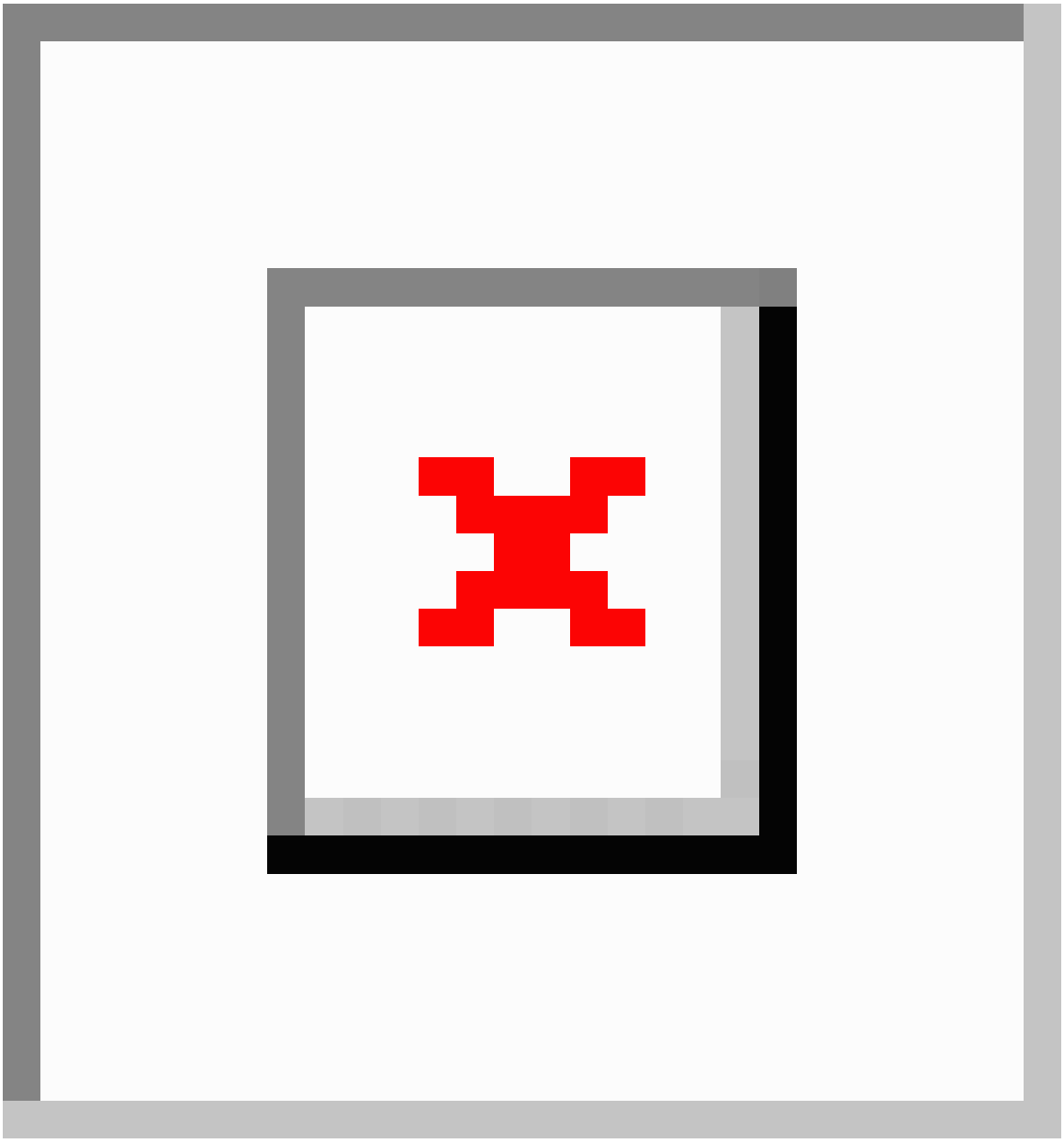
Une fois que le nœud de données a appris les routes du nœud de contrôle, chaque nœud prend des décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée du nœud de contrôle avec les nœuds de données. S'il y a basculement du nœud de contrôle, le routeur voisin détectera un redémarrage; le basculement n'est pas transparent. Le processus OSPF choisit une adresse IP comme ID de routeur. Bien que cela ne soit pas obligatoire, vous pouvez attribuer un ID de routeur statique pour vous assurer qu'un ID de routeur cohérent est utilisé dans la grappe. Consultez la fonctionnalité de transfert sans arrêt OSPF pour gérer l'interruption.

Routage dynamique en mode d'interface individuelle

En mode d'interface individuel, chaque nœud exécute le protocole de routage en tant que routeur autonome, et les routes sont apprises par chaque nœud indépendamment.

Illustration 81 : Routage dynamique en mode d'interface individuelle



Dans le diagramme ci-dessus, le routeur A détecte qu'il existe quatre chemins à coûts égaux vers le routeur B, chacun passant par un nœud. ECMP est utilisé pour équilibrer la charge du trafic entre les quatre chemins. Chaque nœud choisit un ID de routeur différent lorsqu'il communique avec des routeurs externes.

Vous devez configurer un groupement de grappes pour l'ID de routeur afin que chaque nœud ait un ID de routeur distinct.

Le protocole EIGRP ne forme pas de relations de voisinage avec les homologues de la grappe en mode d'interface individuelle.

Remarque Si la grappe comporte plusieurs contiguïtés avec le même routeur à des fins de redondance, le routage dissymétrique peut entraîner une perte de trafic inacceptable. Pour éviter le routage dissymétrique, regroupez toutes ces interfaces de nœud dans la même zone de trafic. Voir Configurer une zone de trafic, à la page 750.

Routage dynamique en mode de contexte multiple

En mode de contexte multiple, chaque contexte gère une table de routage et des bases de données de protocole de routage distinctes. Cela vous permet de configurer les protocoles OSPFv2 et EIGRP indépendamment dans chaque contexte. Vous pouvez configurer le protocole EIGRP dans certains contextes et le protocole OSPFv2 dans le même contexte ou des contextes différents. En mode de contexte mixte, vous pouvez activer n'importe quel protocole de routage dynamique dans les contextes qui sont en mode routé. Les protocoles RIP et OSPFv3 ne sont pas pris en charge en mode de contexte multiple.

Le tableau suivant répertorie les attributs des protocoles EIGRP et OSPFv2, les cartes de routage utilisées pour la distribution des routes dans les processus OSPFv2 et EIGRP, ainsi que les listes de préfixes utilisées dans le protocole OSPFv2 pour filtrer les mises à jour de routage entrant ou sortant d'une zone lorsqu'elles sont utilisées en mode de contexte multiple :

EIGRP	OSPFv2	Cartes de routage et listes de préfixes
Une instance est prise en charge par contexte.	Deux instances sont prises en charge par contexte.	S. O.
Il est désactivé dans le contexte système.		S. O.
Deux contextes peuvent utiliser les mêmes numéros de système autonome ou des numéros différents.	Deux contextes peuvent utiliser des ID de zone identiques ou différents.	S. O.
Les interfaces partagées dans deux contextes peuvent avoir plusieurs instances EIGRP en cours d'exécution.	Les interfaces partagées dans deux contextes peuvent avoir plusieurs instances OSPF en cours d'exécution.	S. O.
L'interaction des instances EIGRP sur les interfaces partagées est prise en charge.	L'interaction des instances OSPFv2 sur les interfaces partagées est prise en charge.	S. O.
Toutes les interfaces de ligne de commande disponibles en mode unique le sont également en mode de contexte multiple.		
Chaque interface de ligne de commande n'a d'effet que dans le contexte dans lequel elle est utilisée.		

Gestion des ressources de routage

Une classe de ressources appelée *routes* spécifie le nombre maximum d'entrées de table de routage pouvant exister dans un contexte. Cela résout le problème d'un contexte affectant les entrées de table de routage

disponibles dans un autre contexte et vous permet également de mieux contrôler le nombre maximum d'entrées de route par contexte.

Comme il n'y a pas de limite système définitive, vous pouvez uniquement spécifier une valeur absolue pour cette limite de ressource; vous ne pouvez pas utiliser de limite de pourcentage. De plus, il n'y a pas de limites minimum et maximum par contexte, de sorte que la classe par défaut ne change pas. Si vous ajoutez une nouvelle route pour l'un des protocoles de routage statique ou dynamique (connecté, statique, OSPF, EIGRP et RIP) dans un contexte et que la limite de ressources pour ce contexte est expirée, l'ajout de route échoue et un message de journal système est généré.

Table de routage pour le trafic de gestion

En tant que pratique de sécurité courante, il est souvent nécessaire de séparer et d'isoler le trafic de gestion (provenant du périphérique) du trafic de données. Pour réaliser cet isolement, le périphérique ASA utilise une table de routage distincte pour le trafic de gestion uniquement par rapport au trafic de données. Des tableaux de routage distincts signifient que vous pouvez créer des routages par défaut distincts pour les données et la gestion.

Types de trafic pour chaque table de routage

Le trafic de l'appareil utilise toujours la table de routage des données.

Le trafic en provenance du périphérique, selon le type, utilise par défaut la table de tourage réservé à la gestion ou la table de routage des données. Si aucune correspondance n'est trouvée dans la table de routage par défaut, il vérifie l'autre table de routage.

- Le trafic de la table de gestion uniquement à partir de l'appareil comprend des fonctionnalités qui ouvrent un fichier distant à l'aide de HTTP, SCP, TFTP, la commande **copy** , les licences Smart, Smart Call Home, **trustpointtrustpool**, etc.
- Le trafic du tableau de données du périphérique comprend toutes les autres fonctionnalités telles que le ping, le DNS, le DHCP, etc.

Interfaces incluses dans la table de routage de gestion uniquement

Les interfaces de gestion uniquement comprennent toutes les interfaces x/x Management (gestion) ainsi que toutes les interfaces que vous avez configurées pour être uniquement de gestion.

Repli vers l'autre table de routage

Si aucune correspondance n'est trouvée dans la table de routage par défaut, il vérifie l'autre table de routage.

Utilisation de la table de routage autre que par défaut

Si vous avez besoin que le trafic initial sorte d'une interface qui ne figure pas dans sa table de routage par défaut, vous devrez peut-être spécifier cette interface lorsque vous la configurerez, plutôt que de vous fier à l'autre table. Le ASA vérifiera uniquement les routes pour l'interface spécifiée. Par exemple, si vous avez besoin d'un ping pour sortir une interface de gestion uniquement, spécifiez l'interface dans la fonction envoyer un message Ping. Sinon, s'il existe une route par défaut dans la table de routage de données, elle correspondra à la route par défaut et ne reviendra jamais à la table de routage de gestion.

Routage dynamique

La table de routage réservé à la gestion prend en charge le routage dynamique distinct de la table de routage de l'interface de données. Un processus de routage dynamique donné doit s'exécuter sur l'interface de gestion uniquement ou sur l'interface de données; vous ne pouvez pas mélanger les deux types. Lors de la mise à niveau à partir d'une version antérieure sans table de routage de gestion distinct, si vous avez un mélange

d'interfaces de données et de gestion utilisant le même processus de routage dynamique, les interfaces de gestion seront abandonnées.

Fonctionnalité d'accès de gestion pour les exigences VPN

Si vous configurez la fonctionnalité d'accès de gestion qui permet l'accès de gestion à une interface autre que celle à partir de laquelle vous avez entré l'ASA lors de l'utilisation du VPN, alors, en raison de considérations de routage avec les tables de gestion et de routage de données distinctes, l'interface de terminaison VPN et la gestion L'interface d'accès doit être du même type : les deux doivent être des interfaces de gestion uniquement ou des interfaces de données standard.

Identification de l'interface de gestion

Une interface configurée avec l'option de gestion uniquement est considérée comme une interface de gestion.

Dans la configuration suivante, les interfaces GigabitEthernet0/0 et Management0/0 sont considérées comme des interfaces de gestion.

```
a/admin(config-if)# show running-config int g0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.10.10.123 255.255.255.0
 ipv6 address 123::123/64
a/admin(config-if)# show running-config int m0/0
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 10.106.167.118 255.255.255.0
a/admin(config-if)#
```

Routage à chemins multiples à coûts égaux (ECMP)

L'ASA prend en charge le routage à chemins multiples à coûts égaux (ECMP).

Vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal par interface. Par exemple, vous pouvez configurer plusieurs routes par défaut sur l'interface externe qui spécifient différentes passerelles.

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

Dans ce cas, le trafic est équilibré en charge sur l'interface externe entre 10.1.1.2, 10.1.1.3 et 10.1.1.4. Le trafic est réparti entre les passerelles précisées selon un algorithme qui procède au hachage des adresses IP source et de destination, de l'interface entrante, du protocole et des ports source et destination.

ECMP sur plusieurs interfaces à l'aide de zones de trafic

Si vous configurez des zones de trafic pour contenir un groupe d'interfaces, vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal sur 8 interfaces au sein de chaque zone. Par exemple, vous pouvez configurer plusieurs routes par défaut sur trois interfaces dans la zone :

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

De même, votre protocole de routage dynamique peut configurer automatiquement des routes à coût égal. L'ASA équilibre la charge du trafic entre les interfaces grâce à un mécanisme d'équilibrage de la charge plus robuste.

Lorsqu'un routage est perdu, le périphérique déplace le flux de manière transparente vers une autre route.

Désactiver les demandes ARP du mandataire

Lorsqu'un hôte envoie du trafic IP à un autre périphérique sur le même réseau Ethernet, l'hôte doit connaître l'adresse MAC du périphérique. ARP est un protocole de couche 2 qui résout une adresse IP en une adresse MAC. Un hôte envoie une demande ARP de type « À qui appartient cette adresse IP? ». Le périphérique qui possède l'adresse IP répond : « Je possède cette adresse IP; voici mon adresse MAC. »

L'ARP du mandataire est utilisé lorsqu'un périphérique répond à une demande ARP avec sa propre adresse MAC, même si le périphérique ne possède pas l'adresse IP. L'ASA utilise un ARP de mandataire lorsque vous configurez la NAT et spécifiez une adresse mappée qui se trouve sur le même réseau que l'interface ASA. Le trafic ne peut atteindre les hôtes que si l'ASA utilise un ARP de mandataire pour revendiquer que l'adresse MAC est attribuée aux adresses mappées de destination.

Dans de rares cas, vous souhaiterez peut-être désactiver l'ARP du mandataire pour les adresses NAT.

Si vous avez un ensemble d'adresses du client VPN qui chevauche un réseau existant, l'ASA envoie par défaut des demandes ARP de mandataire sur toutes les interfaces. Si vous avez une autre interface qui se trouve sur le même domaine de couche 2, elle verra les demandes ARP et répondra par l'adresse MAC de son interface. Il en résulte que le trafic de retour des clients VPN vers les hôtes internes ira à la mauvaise interface et sera abandonné. Dans ce cas, vous devez désactiver les demandes ARP de mandataire pour l'interface sur laquelle vous ne les souhaitez pas.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Proxy ARP/Neighbor Discovery (ARP de mandataire/Découverte de voisin)**.

Le champ Interface répertorie les noms d'interface. Le champ Enabled (Activé) indique si l'option ARP de mandataire/découverte de voisin est activée (Oui) ou désactivée (Non) pour les adresses globales NAT.

Étape 2 Pour activer l'option ARP de mandataire/découverte de voisin pour l'interface sélectionnée, cliquez sur **Enable** (Activer). Par défaut, l'option ARP de mandataire/découverte de voisin est activée pour toutes les interfaces.

Étape 3 Pour désactiver l'option ARP de mandataire/découverte de voisin pour l'interface sélectionnée, cliquez sur **Disable** (Désactiver).

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer vos paramètres dans la configuration d'exécution.

Afficher la table de routage

Pour afficher toutes les routes d'ASDM qui se trouvent dans la table de routage, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **Routes**. Chaque ligne représente une route.

Historique de l'aperçu du routage

Tableau 36 : Historique de l'aperçu du routage

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Table de routage pour l'interface de gestion	9.5(1)	Pour séparer et isoler le trafic de gestion du trafic de données, une table de routage distincte est ajoutée pour le trafic de gestion. Des tables de routage distinctes, pour la gestion et les données respectivement, sont créées pour IPv4 et IPv6, pour chaque contexte, de l'ASA. De plus, pour chaque contexte de l'ASA, deux tables de routage supplémentaires sont ajoutées dans la RIB et la FIB. Nous avons mis à jour les écrans suivants :



CHAPITRE 29

Routages statiques et par défaut

Ce chapitre décrit comment configurer les routes statiques et par défaut sur l'ASA.

- À propos des routages statiques et par défaut, à la page 863
- Lignes directrices pour les routages statiques et par défaut, à la page 865
- Configurer les routes par défaut et statiques, à la page 866
- Supervision d'une route statique ou par défaut, à la page 869
- Exemples de routes statiques ou par défaut, à la page 870
- Historique des routes statiques et par défaut, à la page 870

À propos des routages statiques et par défaut

Pour acheminer le trafic vers un hôte ou un réseau non connecté, vous devez définir une voie de routage vers l'hôte ou le réseau, à l'aide du routage statique ou dynamique. En général, vous devez configurer au moins une route statique : une route par défaut pour tout le trafic qui n'est pas acheminé par d'autres moyens vers une passerelle de réseau par défaut, en général le routeur du saut suivant.

Routage par défaut

L'option la plus simple est de configurer une voie de routage statique par défaut pour envoyer tout le trafic vers un routeur en amont, en se fondant sur le routeur pour acheminer le trafic à votre place. Une voie de routage par défaut identifie l'adresse IP de la passerelle à laquelle ASA envoie tous les paquets IP pour lesquels il n'a pas de voie de routage statique ou apprise. Une voie de routage statique par défaut est simplement une voie de routage statique avec 0.0.0.0/0 (IPv4) ou::/0 (IPv6) comme adresse IP de destination.

Vous devez toujours définir une voie de routage par défaut.

Comme le périphérique ASA utilise des tables de routage distinctes pour le trafic de données et le trafic de gestion, vous pouvez éventuellement configurer une voie de routage par défaut pour le trafic de données et une autre voie de routage par défaut pour le trafic de gestion. Notez que le trafic provenant du périphérique utilise par défaut la table de routage de gestion uniquement ou de données, en fonction du type, mais qu'il revient à l'autre table de routage si aucune route n'est trouvée. Les routes par défaut correspondront toujours au trafic et empêcheront un recours à l'autre table de routage. Dans ce cas, vous devez préciser l'interface que vous souhaitez utiliser pour le trafic de sortie si cette interface ne figure pas dans la table de routage par défaut.

Routes statiques

Vous pourriez souhaiter utiliser des routes statiques dans les cas suivants :

- Vos réseaux utilisent un protocole de découverte de routeur non pris en charge.
- Votre réseau est de petite taille et vous pouvez facilement gérer des routes statiques.
- Vous ne voulez pas associer le trafic ou la surcharge de la CPU aux protocoles de routage.
- Dans certains cas, une route par défaut ne suffit pas. La passerelle par défaut peut ne pas être en mesure d'atteindre le réseau de destination, vous devez donc également configurer des routes statiques plus spécifiques. Par exemple, si la passerelle par défaut est externe, la voie de routage par défaut ne peut pas diriger le trafic vers des réseaux internes qui ne sont pas directement connectés à ASA.
- Vous utilisez une fonctionnalité qui ne prend pas en charge les protocoles de routage dynamique.

Routage vers l'interface null0 pour abandonner le trafic indésirable

Les règles d'accès vous permettent de filtrer les paquets en fonction des informations contenues dans leurs en-têtes. Une voie de routage statique vers l'interface null0 est une solution complémentaire aux règles d'accès. Vous pouvez utiliser une route null0 pour transférer le trafic indésirable ou indésirable afin que le trafic soit abandonné.

Les routes statiques Null0 ont un profil de rendement positif. Vous pouvez également utiliser des routes statiques null0 pour éviter les boucles de routage. BGP peut tirer parti de la route statique null0 pour le routage trou noir déclenché à distance.

Priorités de routage

- Les routes qui identifient une destination spécifique prévalent sur la route par défaut.
- Lorsque plusieurs routages existent vers la même destination (statique ou dynamique), la distance administrative du routage détermine la priorité. Les routes statiques sont définies à 1, ce sont donc généralement les routes les plus prioritaires.
- Lorsque vous avez plusieurs routes statiques vers la même destination avec la même distance administrative, consultez Routage à chemins multiples à coûts égaux (ECMP), à la page 859.
- Pour le trafic sortant d'un tunnel avec l'option tunnelisé, cette voie de routage remplace toute autre voie de routage par défaut configurée ou apprise.

Routages en mode de pare-feu transparent et de groupes de ponts

Pour le trafic qui provient de l'ASA et est destiné à travers une interface membre de groupe de ponts pour un réseau non connecté directement, vous devez configurer une voie de routage par défaut ou des routes statiques pour que l'ASA sache de quelle interface membre de groupe de ponts envoyer trafic. Le trafic provenant de l'ASA peut inclure des communications avec un serveur syslog ou SNMP. Si certains serveurs ne peuvent pas être atteints par une seule route par défaut, vous devez configurer des routes statiques. Pour le mode transparent, vous ne pouvez pas spécifier les BVI comme interface de passerelle; seules les interfaces membres peuvent être utilisées. Pour les groupes de ponts en mode routé, vous devez préciser le BVI dans une voie de

routage statique; vous ne pouvez pas définir d'interface membre. Consultez Recherches d'adresse MAC ou de route, à la page 225 pour de plus amples renseignements.

Suivi du routage statique

L'un des problèmes des routes statiques est qu'il n'y a pas de mécanisme inhérent pour déterminer si la route est active ou inactive. Les routes statiques restent dans la table de routage même si la passerelle du saut suivant n'est plus disponible. Les routes statiques ne sont supprimées de la table de routage que si l'interface associée ASA tombe en panne.

La fonction de suivi de route statique fournit une méthode de suivi de la disponibilité d'une route statique et d'installation d'une route de secours en cas de défaillance de la route principale. Par exemple, vous pouvez définir une route par défaut vers une passerelle de FAI et une route de secours par défaut vers un FAI secondaire au cas où le FAI principal deviendrait indisponible.

L'ASA met en œuvre le suivi de route statique en associant une route statique à un hôte cible de surveillance sur le réseau de destination que l'ASA surveille à l'aide des demandes Echo ICMP. Si aucune réponse écho n'est reçue dans un délai donné, l'hôte est considéré comme hors service et la route associée est supprimée de la table de routage. Une route de secours non suivie avec une métrique plus élevée est utilisée à la place de la route supprimée.

Lorsque vous sélectionnez une cible de surveillance, vous devez vous assurer qu'elle peut répondre aux demandes d'écho ICMP. La cible peut être n'importe quel objet réseau de votre choix, mais vous pouvez envisager d'utiliser les objets suivants :

- L'adresse de la passerelle du FAI, pour la prise en charge du double FAI.
- L'adresse de passerelle du saut suivant, si vous êtes préoccupé par la disponibilité de la passerelle.
- Un serveur sur le réseau cible, tel qu'un serveur syslog, avec lequel l'ASA doit communiquer.
- Un objet réseau persistant sur le réseau de destination

Remarque Un poste de travail qui peut être éteint la nuit n'est pas un bon choix.

Vous pouvez configurer le suivi de routage statique pour les routes définies de manière statique ou pour les routages par défaut obtenus par DHCP ou PPPoE. Vous pouvez uniquement activer les clients PPPoE sur plusieurs interfaces avec le suivi de routage configuré.

Lignes directrices pour les routages statiques et par défaut

Mode de pare-feu et groupes de ponts

- En mode transparent, les routes statiques doivent utiliser l'interface du membre du groupe de ponts comme passerelle; vous ne pouvez pas préciser les BVI.
- En mode routé, vous devez spécifier les BVI comme passerelle; vous ne pouvez pas définir l'interface membre.

- Le suivi de routage statique n'est pas pris en charge pour les interfaces membres des groupes de ponts ou sur les BVI.

Adresse réseau prise en charge

- Le suivi de routage statique n'est pas pris en charge pour IPv6.
- L'ASA ne prend pas en charge le routage de classe E, donc un réseau de classe E n'est pas routable dans les routes statiques.

Mise en grappe et mode de contexte multiple

- Dans la mise en grappe, le suivi de routage statique n'est pris en charge que sur le nœud de contrôle.
- Le suivi de routage statique n'est pas pris en charge en mode de contexte multiple.

Entrées de routage ASP et RIB

Tous les routages et leur distance installés sur le périphérique sont capturés dans la table de routage ASP. Cette situation est commune à tous les protocoles de routage statiques et dynamiques. Seule la meilleure distance de routage est saisie dans le tableau RIB.

Configurer les routes par défaut et statiques

Vous devez configurer au moins une route par défaut. Vous devrez peut-être également configurer des routes statiques. Dans cette section, nous allons configurer une route par défaut, configurer une route statique et suivre une route statique.

Configurer une route par défaut

Une voie de routage par défaut est simplement une voie de routage statique avec 0.0.0.0/0 comme adresse IP de destination. Vous devez toujours avoir une route par défaut, soit configurée manuellement avec cette procédure, soit dérivée d'un serveur DHCP ou d'un autre protocole de routage.

Avant de commencer

Consultez les consignes suivantes pour l'option Tunneled (Tunnélisé) :

- N'activez pas la fonction de monodiffusion RPF sur l'interface de sortie d'une route tunnellisée, car ce paramètre entraîne l'échec de la session.
- N'activez pas l'interception TCP sur l'interface de sortie de la route tunnellisée, car ce paramètre fait échouer la session.
- N'utilisez pas les moteurs d'inspection VoIP (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), la plateforme d'inspection DNS ou la plateforme d'inspection d'appel RPC DCE avec des routes tunnellisées, car ces moteurs d'inspection ignorent la route tunnellisée.
- Vous ne pouvez pas définir plusieurs routes par défaut avec l'option tunnellisée.
- ECMP pour le trafic en tunnel n'est pas pris en charge.

- Les routes tunnellisées ne sont pas prises en charge pour les groupes de ponts, qui ne prennent pas en charge la terminaison VPN pour le trafic traversant.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration des périphériques)** > **Routing (Routage)** > **Static Routes (Routes statiques)**, puis cliquez sur **Add** (Ajouter).

Étape 2 Choisissez l'**IP Address Type** (Type d'adresse IP), **IPv4** ou **IPv6.**

Étape 3 Choisissez l'**Interface** par laquelle vous souhaitez envoyer le trafic.

Pour le mode transparent, spécifiez un nom d'interface de membre de groupe de ponts. Pour le mode routé avec groupes de ponts, spécifiez le nom des BVI.

Étape 4 Pour le **Network** (Réseau), tapez **any4** ou **any6**, selon le type.

Étape 5 Indiquez la **Gateway IP** (Adresse IP de la passerelle) par laquelle vous souhaitez envoyer le trafic.

Étape 6 Renseignez le champ **Metric** (Mesure) pour définir la distance administrative de la route.

La valeur par défaut est **1**. La distance administrative est un paramètre utilisé pour comparer les routes entre différents protocoles de routage. La distance administrative par défaut pour les routes statiques est de 1, ce qui lui donne priorité sur les routes découvertes par les protocoles de routage dynamique, mais pas sur les routes directement connectées. La distance administrative par défaut pour les routes découvertes par OSPF est de 110. Si une route statique a la même distance administrative qu'une route dynamique, les routes statiques prévalent. Les routes connectées ont toujours la priorité sur les routes statiques ou découvertes dynamiquement.

Étape 7 (Facultatif) Dans la zone **Options**, définissez les options suivantes :

- **Tunneled** (Tunnélisé) : vous pouvez définir une route par défaut distincte pour le trafic VPN si vous souhaitez que votre trafic VPN utilise une route par défaut différente de celle du trafic non VPN. Par exemple, le trafic entrant des connexions VPN peut être facilement dirigé vers les réseaux internes, tandis que le trafic des réseaux internes peut être dirigé vers l'extérieur. Lorsque vous créez une route par défaut avec l'option tunnelisé, tout le trafic provenant d'un tunnel se terminant sur l'ASA qui ne peut pas être acheminé à l'aide de routes apprises ou statiques est envoyé vers cette route. Cette option n'est pas prise en charge pour les groupes de ponts.
- **Tracked** (Suivi) : (IPv4 uniquement) Pour en savoir plus sur le suivi des routes, consultez Configurer le suivi de route statique, à la page 868.

Étape 8 Cliquez sur **OK**.

Configurer une route statique

Une voie de routage statique définit où envoyer le trafic pour des réseaux de destination spécifiques.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration des périphériques)** > **Routing (Routage)** > **Static Routes (Routes statiques)**, puis cliquez sur **Add** (Ajouter).

Étape 2 Choisissez l'**IP Address Type** (Type d'adresse IP), **IPv4** ou **IPv6.**

Étape 3 Choisissez l'**Interface** par laquelle vous souhaitez envoyer le trafic.

Pour abandonner le trafic indésirable, choisissez l'interface **Null0**. Pour le mode transparent, spécifiez un nom d'interface de membre de groupe de ponts. Pour le mode routé avec groupes de ponts, spécifiez le nom des BVI.

Étape 4 Pour le **Network** (Réseau), saisissez le réseau de destination pour lequel vous souhaitez acheminer le trafic.

Étape 5 Indiquez la **Gateway IP** (Adresse IP de la passerelle) par laquelle vous souhaitez envoyer le trafic.

Étape 6 Renseignez le champ **Metric** (Mesure) pour définir la distance administrative de la route.

La valeur par défaut est **1**. La distance administrative est un paramètre utilisé pour comparer les routes entre différents protocoles de routage. La distance administrative par défaut pour les routes statiques est de 1, ce qui lui donne priorité sur les routes découvertes par les protocoles de routage dynamique, mais pas sur les routes directement connectées. La distance administrative par défaut pour les routes découvertes par OSPF est de 110. Si une route statique a la même distance administrative qu'une route dynamique, les routes statiques prévalent. Les routes connectées ont toujours la priorité sur les routes statiques ou découvertes dynamiquement.

Étape 7 (Facultatif) Dans la zone **Options**, définissez les options suivantes :

- **Tunneled** (Tunnélisé) : vous pouvez définir une route par défaut distincte pour le trafic VPN si vous souhaitez que votre trafic VPN utilise une route par défaut différente de celle du trafic non VPN. Par exemple, le trafic entrant des connexions VPN peut être facilement dirigé vers les réseaux internes, tandis que le trafic des réseaux internes peut être dirigé vers l'extérieur. Lorsque vous créez une route par défaut avec l'option tunnelisé, tout le trafic provenant d'un tunnel se terminant sur l'ASA qui ne peut pas être acheminé à l'aide de routes apprises ou statiques est envoyé vers cette route.
- **Tracked** (Suivi) : (IPv4 uniquement) Pour en savoir plus sur le suivi des routes, consultez Configurer le suivi de route statique, à la page 868.

Étape 8 Cliquez sur **OK**.

Configurer le suivi de route statique

Pour configurer le suivi des routes statiques, procédez comme suit.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Static Routes (Routes statiques)** et ajoutez ou modifiez une route statique conformément à Configurer une route statique, à la page 867.

Étape 2 Cliquez sur le bouton radio **Tracked** (Suivi) dans la zone **Options**.

Étape 3 Dans le champ **Track ID** (ID de suivi), saisissez un identifiant unique pour le processus de suivi de routage.

Étape 4 Dans le champ **Track IP Address/DNS Name** (Suivre l'adresse IP/le nom DNS), saisissez l'adresse IP ou le nom d'hôte de la cible suivie. En règle générale, il s'agit de l'adresse IP de la passerelle de saut suivant pour le routage, mais il peut s'agir de tout objet réseau disponible depuis cette interface.

Étape 5 Dans le champ **SLA ID** (ID de SLA), saisissez un identifiant unique pour le processus de supervision des SLA.

Étape 6 (Facultatif) Cliquez sur **Monitoring Options** (Options de surveillance).

La boîte de dialogue **Route Monitoring Options** (Options de surveillance du routage) apparaît. À partir de là, modifiez les propriétés de surveillance de l'objet de suivi suivantes :

- **Frequency** (Fréquence) : définit la fréquence, en secondes, à laquelle l'ASA doit tester la présence de la cible de suivi. Les valeurs valides vont de 1 à 604800 secondes. La valeur par défaut est 60 secondes.
- **Threshold** (Seuil) : définit la durée, en millisecondes, qui indique un événement de dépassement de seuil. Cette valeur ne peut pas être supérieure à la valeur du délai d'expiration.
- **Timeout** (Délai d'expiration) : définit le temps, en millisecondes, pendant lequel l'opération de surveillance du routage doit attendre une réponse des paquets de demande. Les valeurs valides sont comprises entre 0 et 604800000 millisecondes. La valeur par défaut est de 5000 millisecondes.
- **Data Size** (Taille des données) : définit la taille de la charge utile de données à utiliser dans les paquets de demande d'écho. La valeur par défaut est 28. Les valeurs valides sont comprises entre 0 et 16384.



Remarque Ce paramètre spécifie la taille de la charge utile uniquement; il ne spécifie pas la taille du paquet entier.

- **ToS** : définit une valeur pour le type d'octet de service dans l'en-tête IP de la demande d'écho. Les valeurs valides sont comprises entre 0 et 255. La valeur par défaut est 0.
- **Number of Packets** (Nombre de paquets) : définit le nombre de demandes d'écho à envoyer pour chaque test. Les valeurs valides sont comprises entre 1 et 100. La valeur par défaut est 1.

Cliquez sur **OK**.

Étape 7 Cliquez sur **OK** pour enregistrer votre route, puis cliquez sur **Apply** (Appliquer).

Le processus de surveillance commence dès que vous appliquez la route suivie.

Étape 8 Créez une route de secours non suivie.

La route de secours est une route statique vers la même destination que la route suivie, mais via une interface ou une passerelle différente. Vous devez attribuer à cette route une distance administrative (mesure) plus élevée que votre route suivie.

Supervision d'une route statique ou par défaut

- **Monitoring (Supervision) > Routing (Routage) > Routes**.

Dans le volet **Routes**, chaque ligne représente une route. Vous pouvez filtrer par connexions IPv4, connexions IPv6 ou les deux. Les renseignements de routage comprennent le protocole, le type de route, l'adresse IP de destination, la longueur du masque réseau ou du préfixe, l'adresse IP de la passerelle, l'interface par laquelle la route est connectée et la distance administrative.

Exemples de routes statiques ou par défaut

L'exemple suivant montre comment créer une route statique qui envoie tout le trafic destiné à 10.1.1.0/24 au routeur 10.1.2.45, qui est connecté à l'interface interne, définit trois routes statiques à coût égal qui dirigent le trafic vers trois passerelles différentes sur l'interface DMZ, et ajoute une route par défaut pour le trafic tunnelé et une autre pour le trafic normal.

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

Historique des routes statiques et par défaut

Tableau 37 : Historique des fonctionnalités pour les routes statiques et par défaut

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Suivi du routage statique	7.2(1)	La fonction de suivi de route statique fournit une méthode de suivi de la disponibilité d'une route statique et d'installation d'une route de secours en cas de défaillance de la route principale. Nous avons introduit ou modifié les écrans suivants : **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Static Routes (Routes statiques) > Add Static Route Configuration (Ajouter une configuration de route statique) > Device Setup (Configuration de l'appareil) > Routing (Routage) > Static Routes (Routes statiques) > Add Static Route (Ajouter une route statique) > Route Monitoring Options (Options de supervision des routes)**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Route statique null0 pour abandonner le trafic	9.2(1)	L'envoi du trafic vers une interface null0 entraîne l'abandon des paquets destinés au réseau spécifié. Cette fonctionnalité est utile dans la configuration de Remotely Triggered Black Hole (RTBH) pour BGP. Nous avons modifié l'écran suivant : **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Static Routes (Routes statiques) > Add Static Route (Ajouter une route statique)**



CHAPITRE 30

Routage basé sur une stratégie

Ce chapitre décrit comment configurer l'ASA pour prendre en charge le routage basé sur les politiques (BPR). Les sections suivantes décrivent le routage basé sur les politiques, les lignes directrices relatives au PBR et la configuration du PBR.

- À propos du routage basé sur les politiques, à la page 873
- Lignes directrices pour le routage basé sur des politiques, à la page 875
- Configurer le routage basé sur les politiques, à la page 877
- Historique du routage basé sur des politiques, à la page 880

À propos du routage basé sur les politiques

Le routage traditionnel est basé sur la destination, ce qui signifie que les paquets sont acheminés en fonction de l'adresse IP de destination. Cependant, il est difficile de modifier le routage d'un trafic spécifique dans un système de routage basé sur la destination. Avec le routage basé sur les politiques (PBR), vous pouvez définir le routage en fonction de critères autres que le réseau de destination. Le PBR vous permet d'acheminer le trafic en fonction de l'adresse source, du port source, de l'adresse de destination, du port de destination, du protocole ou d'une combinaison de ces éléments.

Routage basé sur les politiques :

- Vous permet de fournir une qualité de service (QoS) à un trafic différencié.
- Vous permet de répartir le trafic interactif et par lots sur des chemins permanents à faible bande passante et à faible coût et des chemins commutés à bande passante élevée et à coût élevé.
- Permet aux fournisseurs de services Internet et à d'autres organisations d'acheminer le trafic provenant de divers ensembles d'utilisateurs par le biais de connexions Internet bien définies.

Le routage basé sur les politiques peut mettre en œuvre la QoS en classant et en marquant le trafic à la périphérie du réseau, puis en utilisant le PBR dans tout le réseau pour acheminer le trafic marqué le long d'un chemin spécifique. Cela permet le routage de paquets provenant de différentes sources vers différents réseaux, même lorsque les destinations sont les mêmes, et cela peut être utile pour interconnecter plusieurs réseaux privés.

Pourquoi utiliser le routage basé sur des politiques?

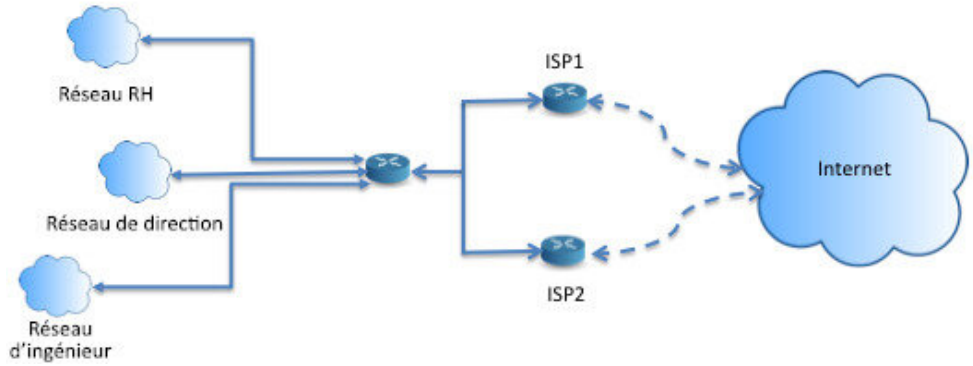
Imaginez une entreprise qui dispose de deux liaisons entre des sites : l'une, une liaison onéreuse à bande passante élevée et à faible délai, et l'autre, à faible bande passante, avec un délai plus élevé et un moindre

coût. Lors de l'utilisation de protocoles de routage traditionnels, la liaison à plus grande largeur de bande recevrait la majeure partie, voire la totalité, du trafic qui y est envoyé, en fonction des économies de métriques obtenues grâce aux caractéristiques de la bande passante et/ou du délai (avec EIGRP ou OSPF) de la liaison. PBR vous permet d'acheminer le trafic de priorité supérieure sur la liaison à bande passante élevée/faible délai, tout en envoyant tout le reste du trafic sur la liaison à bande passante faible/délai élevé.

Certaines applications du routage basé sur les politiques sont les suivantes :

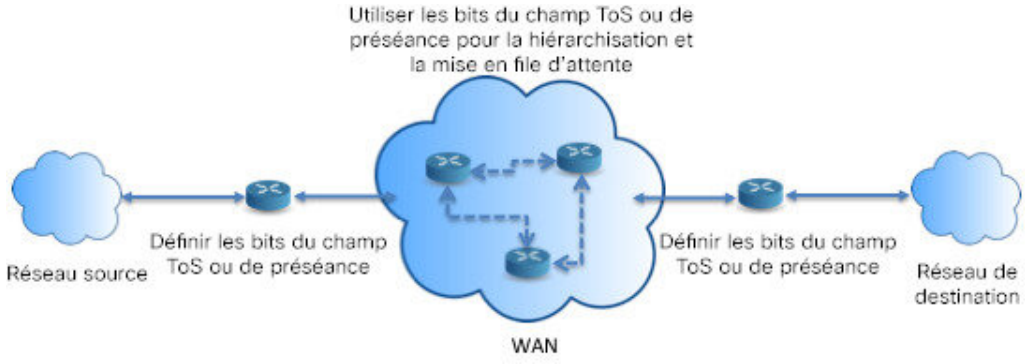
Routage à accès égal et sensible à la source

Dans cette topologie, le trafic provenant du réseau RH et du réseau de gestion peut être configuré pour passer par FAI1, et le trafic du réseau des ingénieurs peut être configuré pour passer par FAI2. Ainsi, le routage basé sur les politiques permet aux administrateurs réseau de fournir un routage à accès égal et sensible à la source, comme indiqué ici.



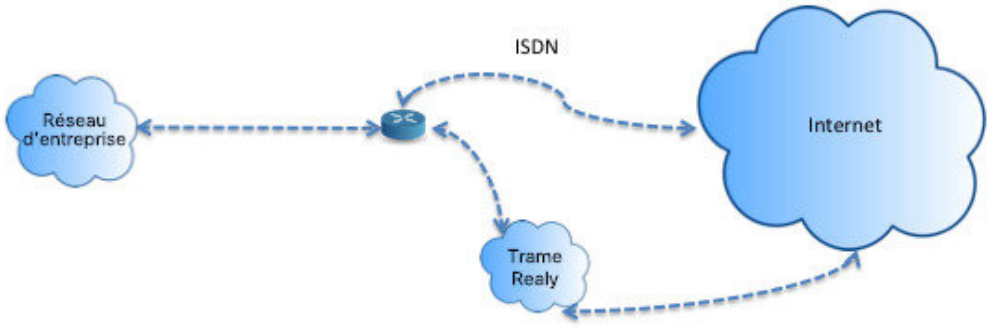
Qualité de service

En balisant les paquets avec le routage basé sur les politiques, les administrateurs réseau peuvent classer le trafic réseau au périmètre du réseau pour différentes classes de service, puis mettre en œuvre ces classes de service au cœur du réseau à l'aide de la mise en file d'attente de priorité, personnalisée ou pondérée (comme indiqué dans la figure ci-dessous). Cette configuration améliore les performances du réseau en éliminant le besoin de classer le trafic explicitement sur chaque interface WAN au cœur du réseau fédérateur.



Réduction des coûts

Une organisation peut diriger le trafic en bloc associé à une activité spécifique pour utiliser un lien à haute bande passante à coût élevé pendant une durée courte et maintenir la connectivité de base sur un lien à faible coût à bande passante inférieure pour le trafic interactif en définissant la topologie, comme indiqué ici.



Partage de la charge

En plus des fonctionnalités de partage dynamique de charge offertes par l'équilibrage de charge ECMP, les administrateurs réseau peuvent désormais mettre en œuvre des politiques pour répartir le trafic entre plusieurs chemins en fonction des caractéristiques du trafic.

Par exemple, dans la topologie décrite dans le scénario de routage à accès égalitaire sensible, un administrateur peut configurer le routage basé sur une politique pour partager la charge du trafic provenant du réseau des Ressources humaines par ISP1 et du trafic provenant du réseau Eng par ISP2.

Mise en œuvre de PBR

L'ASA utilise les ACL pour faire correspondre le trafic et effectuer des actions de routage sur le trafic. Plus précisément, vous configurez une carte de routage qui spécifie une ACL pour la correspondance, puis vous spécifiez une ou plusieurs actions pour ce trafic. Enfin, vous associez la carte de routage à une interface sur laquelle vous souhaitez appliquer le PBR à tout le trafic entrant.

Remarque Avant de procéder à la configuration, assurez-vous que le trafic d'entrée et de sortie de chaque session traverse la même interface destinée au fournisseur de services Internet pour éviter les comportements imprévus causés par le routage asymétrique, en particulier lorsque la NAT et le VPN sont utilisés.

Lignes directrices pour le routage basé sur des politiques

Mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Routage par flux

Étant donné que l'ASA effectue le routage par flux, le routage des politiques est appliqué sur le premier paquet et la décision de routage qui en résulte est stockée dans le flux créé pour le paquet. Tous les paquets suivants appartenant à la même connexion correspondent simplement à ce flux et sont acheminés de manière appropriée.

Politiques PBR non appliquées pour la recherche de route de sortie

Le routage basé sur des règles est une fonction d'entrée uniquement, c'est-à-dire qu'il n'est appliqué qu'au premier paquet d'une nouvelle connexion entrante, et c'est à ce moment-là que l'interface de sortie est sélectionnée pour le tronçon d'aller de la connexion. Notez que PBR ne sera pas déclenché si le paquet entrant appartient à une connexion existante ou si la NAT est appliquée et que cette dernière choisit l'interface de sortie.

Politiques PBR non appliquées pour le trafic amorce



Remarque Il y a connexion amorce lorsque l'établissement de liaison nécessaire entre la source et la destination n'a pas lieu.

Lorsqu'une nouvelle interface interne est ajoutée et qu'une nouvelle politique VPN est créée à l'aide d'un groupement d'adresses unique, le PBR est appliqué à l'interface externe correspondant à la source du nouveau groupement de clients. Ainsi, PBR envoie le trafic du client au prochain saut sur la nouvelle interface. Cependant, PBR n'est pas impliqué dans le trafic de retour d'un hôte qui n'a pas encore établi de connexion avec les nouvelles routes d'interface interne vers le client. Ainsi, le trafic de retour de l'hôte vers le client VPN, en particulier la réponse du client VPN, est abandonné car il n'y a aucune voie de routage valide. Vous devez configurer une voie de routage statique pondérée avec une métrique plus élevée sur l'interface interne.

Mise en grappe

- La mise en grappe est prise en charge.
- Dans un scénario de grappe, sans routes statiques ou dynamiques, et avec la commande ip-verify-reverse path activée, le trafic asymétrique peut être abandonné. Il est donc conseillé de désactiver ip-verify-reverse path.

Prise en charge d'IPv6

IPv6 est pris en charge.

Lignes directrices relatives à la surveillance des chemins d'accès

Voici les lignes directrices pour configurer la surveillance des chemins d'accès sur les interfaces :

- Les interfaces doivent avoir un nom d'interface.
- Les interfaces de gestion uniquement ne peuvent pas être configurées avec la surveillance des chemins d'accès. Pour configurer la surveillance des chemins d'accès, vous devez décocher la case **Dedicate this interface to management only** (Dédier cette interface à la gestion uniquement).
- La surveillance des chemins d'accès n'est pas prise en charge sur les périphériques en mode de système transparent ou de contexte multiple.

- Les types de surveillance automatique (auto, auto4 et auto6) ne sont pas pris en charge pour les interfaces de tunnel.
- La surveillance des chemins d'accès ne peut pas être configurée pour les interfaces suivantes :
  - BVI
  - Boucle avec retour
  - DVTI

Directives supplémentaires

- Toutes les restrictions et limites de configuration existantes liées aux cartes de routage seront conservées.
- N'utilisez pas de cartes de routage contenant des listes de correspondance de politiques pour le routage basé sur des politiques. La liste de politiques de correspondance est uniquement utilisée pour le BGP.
- Le transfert de chemin inverse de monodiffusion (uRPF) valide l'adresse IP source des paquets reçus sur une interface par rapport à la table de routage et non par rapport à la carte de routage PBR. Lorsque uRPF est activé, les paquets reçus sur une interface par l'intermédiaire de PBR sont abandonnés tels qu'ils sont, sans l'entrée de route spécifique. Par conséquent, lorsque vous utilisez PBR, assurez-vous de désactiver uRPF.

Configurer le routage basé sur les politiques

Une carte de routage est composée d'une ou de plusieurs instructions route-map. Chaque instruction a un numéro de séquence, ainsi qu'une clause allow ou deny. Chaque instruction route-map contient des commandes match et set. La commande match indique les critères de correspondance à appliquer au paquet. La commande set indique l'action à entreprendre sur le paquet.

- Lorsqu'une carte de routage est configurée avec des clauses match/set IPv4 et IPv6 ou lorsqu'une ACL unifiée faisant correspondre le trafic IPv4 et IPv6 est utilisée, les actions définies seront appliquées en fonction de la version IP de destination.
- Lorsque plusieurs interfaces ou sauts suivants sont configurés en tant qu'action définie, toutes les options sont évaluées l'une après l'autre jusqu'à ce qu'une option utilisable valide soit trouvée. Aucun équilibrage de charge ne sera effectué parmi les multiples options configurées.
- L'option verify-availability n'est pas prise en charge en mode de contexte multiple.

Procédure

Étape 1 Dans ASDM, configurez une ou plusieurs ACL standard ou étendues pour identifier le trafic sur lequel vous souhaitez effectuer le routage basé sur les politiques. Voir **Configuration de** > **gestionnaire avancé d'ACL du** > **pare-feu** > .

Étape 2 Choisissez **Configuration** > **Device Setup (Configuration des périphériques)** > **Routing (routage)** > **Route Maps (carte de routage)**, et cliquez sur **Add** (Ajouter).

La boîte de dialogue**Add Route map** (Ajouter une carte de routage) apparaît.

Étape 3 Saisissez le nom et le numéro de séquence de la carte de routage. Vous utiliserez ce même nom pour des instructions de carte de routage supplémentaires facultatives. Le numéro de séquence est l'ordre dans lequel ASA évalue les cartes de routage.

Étape 4 Cliquez sur **Deny** (Refuser) ou **Allow** (Autoriser).

La liste de contrôle d'accès comprend également ses propres instructions d'autorisation et de refus. Pour les correspondances Autoriser/Autoriser entre la carte de routage et la liste de contrôle d'accès, le traitement de routage basé sur les politiques se poursuit. Pour les correspondances Autoriser/refuser, le traitement se termine pour cette carte de routage et les autres cartes de routage sont vérifiées. Si le résultat est toujours Autoriser/refuser, la table de routage normale est utilisée. Pour les correspondances refus/refus, le traitement de routage basé sur les politiques se poursuit.

Étape 5 Cliquez sur l'onglet **Map Clause** (Clause relative à la carte) pour identifier les listes de contrôle d'accès que vous avez créées.

Dans la section **IPv4**, choisissez **Access List** (liste d'accès) dans le menu déroulant, puis sélectionnez une ou plusieurs ACL standard ou étendues dans la boîte de dialogue.



Remarque Vérifiez que la liste d'accès ne contient aucune règle inactive. Vous ne pouvez pas définir une correspondance ACL avec les règles inactives sur un PBR.

Si vous utilisez une liste de contrôle d'accès standard, la mise en correspondance s'effectue uniquement pour l'adresse de destination. Si vous utilisez une liste de contrôle d'accès étendue, vous pouvez mettre en correspondance la source, la destination ou les deux.

Utilisez la section IPv4 pour les listes de contrôle d'accès IPv4 et IPv6. Pour la liste de contrôle d'accès étendue, vous pouvez spécifier les paramètres IPv4, IPv6, Identity Firewall ou Cisco TrustSec. Vous pouvez également inclure des objets de service réseau. Pour obtenir la syntaxe complète, consultez la référence de commande ASA.

Étape 6 Cliquez sur l'onglet **Policy Based Routing** (Routage basé sur des politiques) pour définir la politique à appliquer aux flux de trafic.

Cochez une ou plusieurs des actions suivantes à effectuer pour les flux de trafic correspondants :

- **Définir l'adresse IP de saut suivant PBR** : Pour IPv4 et IPv6, vous pouvez configurer plusieurs adresses IP de saut suivant, auquel cas elles sont évaluées dans l'ordre spécifié jusqu'à ce qu'une adresse IP de saut suivant routable soit trouvée. Les prochains sauts configurés doivent être connectés directement; Sinon, l'action définie ne sera pas appliquée.
- **Définir l'adresse IP du saut suivant par défaut :** pour IPv4 et IPv6, si la recherche normale de route échoue pour le trafic correspondant, l'ASA transfère le trafic en utilisant cette adresse IP de saut suivant spécifiée.
- **Trouver et définir de manière récursive l'adresse IP de saut suivant** : l'adresse de saut suivant et l'adresse de saut suivant par défaut exigent que le prochain saut se trouve sur un sous-réseau directement connecté. Avec cette option, l'adresse de saut suivant n'a pas besoin d'être connectée directement. Au lieu de cela, une recherche récursive est effectuée sur l'adresse de saut suivant, et le trafic correspondant est transmis au saut suivant utilisé par cette entrée de routage en fonction du chemin de routage utilisé sur le routeur.
- **Configuration de la vérifiabilité du saut suivant** : vérifie si les prochains sauts IPv4 d'une carte de routage sont disponibles. Vous pouvez configurer un objet de suivi de moniteur SLA pour vérifier

l'accessibilité du prochain saut. Cliquez sur **Add** pour ajouter des entrées d'adresse IP du saut suivant et spécifiez les informations suivantes.

- **Numéro de séquence** : les entrées sont évaluées dans l'ordre à l'aide du numéro de séquence.
- **Adresse IP** : saisissez l'adresse IP.
- **ID d'objet de suivi** : saisissez un ID valide.

- **Définir les interfaces** : cette option configure l'interface par laquelle le trafic correspondant est acheminé. Vous pouvez configurer plusieurs interfaces, auquel cas elles sont évaluées dans l'ordre spécifié jusqu'à ce qu'une interface valide soit trouvée. Lorsque vous spécifiez **null0**, tout le trafic correspondant à la carte de routage sera abandonné. Il doit y avoir une voie de routage pour la destination qui peut être acheminée par l'interface spécifiée (statique ou dynamique).
- **Définir la clause** > **Coût de l'interface adaptative** : cette option se trouve dans l'onglet Set Clause (Définir a clause) plutôt que dans l'onglet **Policy Based Routing** (Routage basé sur une politique). Cette option définit l'interface de sortie en fonction de son coût. Cliquez dans le champ **Available Interfaces** (interfaces disponibles) et sélectionnez les interfaces à prendre en compte. L'interface de sortie est sélectionnée dans la liste des interfaces. Si les coûts des interfaces sont les mêmes, il s'agit d'une configuration active-active et les paquets sont équilibrés (round robin) sur les interfaces de sortie. Si les coûts sont différents, l'interface avec le coût le plus faible est sélectionnée. Les interfaces ne sont prises en compte que si elles sont actives.
- **Définir l'interface null0 comme interface par défaut** : si une recherche de route normale échoue, l'ASA transfère le trafic null0 et le trafic sera abandonné.
- **Définir le bit de non-fragmentation sur 1 ou 0**) : sélectionnez le bouton radio approprié.
- **Définir la valeur du point de code de service différentiel (DSCP) en bits de QoS** : sélectionnez une valeur dans la liste déroulante IPv4 ou IPv6.

Étape 7 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Étape 8 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** (Configuration > Configuration du périphérique > paramètres de l'interface > Interfaces) et configurez les interfaces d'entrée qui doivent appliquer cette carte de routage pour déterminer les interfaces de sortie.

a) Sélectionnez une interface d'entrée , puis cliquez sur **Edit** Modifier).
b) Dans **Route Map**, sélectionnez la carte de routage basée sur les politiques qui doit être appliquée.
c) Si vous avez utilisé le **coût d'interface adaptatif** pour sélectionner l'interface de sortie dans la carte de routage, définissez la valeur du **coût** sur l'interface.

   La valeur peut être 1 à 65535. La valeur par défaut est 0, que vous pouvez réinitialiser en supprimant la valeur de ce champ. Plus le numéro de priorité est faible, plus la priorité est élevée. Par exemple, 1 a priorité sur 2.

d) Pour que PBR utilise des mesures flexibles pour identifier le meilleur chemin pour le routage des paquets, dans la liste déroulante **Path Monitoring** (surveillance des chemins), sélectionnez le type de surveillance approprié :

   - **auto** : envoie des sondes ICMP à la passerelle IPv4 par défaut de l'interface, si elle existe (identique à Auto IPv4). Sinon, envoie à la passerelle par défaut IPv6 de l'interface (identique à Auto IPv6).
   - **ipv4** : envoie les sondes ICMP à l'adresse IPv4 homologue spécifiée (IP du saut suivant) pour la surveillance. Si vous sélectionnez cette option, le champ adjacent est activé. Saisissez l'adresse IPv4 dans le champ.

- **ipv6** : envoie les sondes ICMP à l'adresse IPv4 homologue spécifiée (IP du saut suivant) pour la surveillance. Si vous sélectionnez cette option, le champ adjacent est activé. Saisissez l'adresse IPv4 dans le champ.
- **auto4** : envoie des sondes ICMP à la passerelle IPv4 par défaut de l'interface.
- **auto6** : envoie des sondes ICMP à la passerelle par défaut IPv6 de l'interface.
- **Aucune** : pour désactiver la surveillance des chemins pour l'interface.

e) Cliquez sur **OK**, puis sur **Apply**(appliquer).

Historique du routage basé sur des politiques

Tableau 38 : Historique des cartes de routage

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Indicateurs de supervision des chemins d'accès dans PBR.	9.18(1)	PBR utilise les mesures pour déterminer le meilleur chemin (interface de sortie) pour transférer le trafic. La supervision des chemins informe périodiquement PBR de l'interface surveillée dont la métrique a été modifiée. PBR récupère les dernières valeurs de métrique pour les interfaces surveillées à partir de la base de données de surveillance des chemins et met à jour le chemin d'accès des données. Écrans nouveaux ou modifiés : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage basé sur les politiques	9.4(1)	Le routage basé sur les politiques (PBR) est un mécanisme par lequel le trafic est acheminé par des chemins spécifiques avec une QoS spécifiée à l'aide d'ACL. Les ACL permettent de classer le trafic en fonction du contenu des en-têtes de couche 3 et de couche 4 du paquet. Cette solution permet aux administrateurs de fournir une QoS à un trafic différencié, de répartir le trafic interactif et par lots entre des chemins permanents à faible bande passante et à faible coût et des chemins commutés à bande passante élevée et à coût élevé, et permet aux fournisseurs de services Internet et à d'autres organisations d'acheminer le trafic provenant de divers ensembles d'utilisateurs par le biais de connexions Internet bien définies. Nous avons mis à jour les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage) > Policy Based Routing (Routage basé sur les politiques), Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Interface Settings (Paramètres d'interface) > Interfaces
Prise en charge d'IPv6 pour le routage basé sur les politiques	9.5(1)	Les adresses IPv6 sont désormais prises en charge pour le routage basé sur les politiques. Nous avons modifié les écrans suivants : **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage) > Add Route Map (Ajouter une carte de routage) > Policy Based Routing (Routage basé sur les politiques) Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage) > Add Route Maps (Ajouter des cartes de routage) > Match Clause (Clause de correspondance)**
Prise en charge de VXLAN pour le routage basé sur les politiques	9.5(1)	Vous pouvez maintenant activer le routage basé sur les politiques sur une interface VNI. Nous avons modifié l'écran suivant : **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier une interface) > General (Général)**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge du routage basé sur les politiques pour le pare-feu d'identité et Cisco TrustSec	9.5(1)	Vous pouvez configurer le pare-feu d'identité et Cisco TrustSec, puis utiliser les ACL du pare-feu d'identité et Cisco TrustSec dans les cartes de routage basées sur les politiques. Nous avons modifié l'écran suivant : **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage) > Add Route Maps (Ajouter des cartes de routage) > Match Clause (Clause de correspondance)**



CHAPITRE 31

Cartes de routage

Ce chapitre décrit comment configurer et personnaliser les cartes de routage pour l'ASA.

- À propos des cartes de routage, à la page 883
- Lignes directrices relatives aux cartes de routage, à la page 885
- Définir une carte de routage, à la page 885
- Personnaliser une carte de routage, à la page 888
- Exemple de cartes de routage, à la page 891
- Historique des cartes de routage, à la page 892

À propos des cartes de routage

Les cartes de routage sont utilisées lors de la redistribution des routes dans un processus de routage OSPF, RIP, EIGRP ou BGP. Elles sont également utilisées lors de la génération d'une route par défaut dans un processus de routage. Une carte de routage définit les routes du protocole de routage spécifié qui peuvent être redistribuées dans le processus de routage cible.

Les cartes de routage ont de nombreuses caractéristiques en commun avec les listes de contrôle d'accès bien connues. Voici quelques-unes des caractéristiques communes aux deux :

- Il s'agit d'une séquence ordonnée d'instructions individuelles, et chacune a un résultat d'autorisation ou de refus. L'évaluation d'une liste de contrôle d'accès ou d'une carte de routage comprend une analyse de liste, dans un ordre prédéterminé, et une évaluation des critères de chaque énoncé qui correspond. Une analyse de liste est abandonnée une fois que la première correspondance d'instruction est trouvée et qu'une action associée à la correspondance d'instruction est effectuée.
- Ce sont des mécanismes génériques. Les correspondances de critères et l'interprétation des correspondances sont dictées par la façon dont elles sont appliquées et par la fonctionnalité qui les utilise. Une carte de routage appliquée à différentes entités peut être interprétée différemment.

Voici quelques-unes des différences entre les cartes de routage et les listes de contrôle d'accès :

- Les cartes de routage sont plus flexibles que les listes de contrôle d'accès et peuvent vérifier les routages en fonction de critères que les listes de contrôle d'accès ne peuvent pas vérifier. Par exemple, une carte de routage peut vérifier si le type de routage est interne.
- Chaque liste de contrôle d'accès se termine par une instruction de refus implicite, par convention de conception. Si la fin d'une carte de routage est atteinte pendant les tentatives de mise en correspondance, le résultat dépend de l'application spécifique de la carte de routage. Les cartes de routage appliquées à

la *redistribution* se comportent de la même manière que les listes de contrôle d'accès : si la route ne correspond à aucune clause d'une carte de routage, la redistribution de la route est refusée, comme si la carte de routage contient une déclaration de refus à la fin.

Clauses d'autorisation et de refus

Les cartes de routage peuvent avoir des clauses d'autorisation et de refus. La clause deny rejette les correspondances de routage de la redistribution. Vous pouvez utiliser une liste de contrôle d'accès comme critère de correspondance dans la carte de routage. Étant donné que les listes de contrôle d'accès ont également des clauses d'autorisation et de refus, les règles suivantes s'appliquent lorsqu'un paquet correspond à la liste de contrôle d'accès :

- ACL permit + route map permit : les routes sont redistribuées.
- ACL permit + route map deny : les routes ne sont pas redistribuées.
- ACL deny + route map permit or deny : la clause route-map n'est pas mise en correspondance et la prochaine clause route-map est évaluée.

Valeurs de clause de correspondance et de définition

Chaque clause de carte de routage a deux types de valeurs :

- Une valeur de correspondance sélectionne les routages auxquels cette clause doit être appliquée.
- Une valeur définie modifie les renseignements qui seront redistribués dans le protocole cible.

Pour chaque voie de routage qui est redistribuée, le routeur évalue d'abord les critères de correspondance d'une clause de la carte de routage. Si les critères de correspondance sont réussis, la route est redistribuée ou rejetée comme l'exige la clause allow ou deny , et certains de ses attributs peuvent être modifiés par les valeurs définies à partir des commandes set . Si les critères de correspondance échouent, cette clause ne s'applique pas à la voie de routage et le logiciel procède à l'évaluation de la voie de routage en fonction de la clause suivante de la carte de routage. L'analyse de la carte de routage se poursuit jusqu'à ce qu'une clause correspondant à la route soit trouvée ou jusqu'à ce que la fin de la carte de routage soit atteinte.

Une correspondance ou une valeur définie dans chaque clause peut être manquée ou répétée plusieurs fois, si l'une de ces conditions est remplie :

- Si plusieurs entrées de correspondance sont présentes dans une clause, elles doivent toutes réussir pour une route donnée afin que cette route corresponde à la clause (c'est-à-dire que l'algorithme AND logique est appliqué pour plusieurs commandes de correspondance).
- Si une entrée de correspondance fait référence à plusieurs objets dans une seule entrée, l'un ou l'autre doit correspondre (l'algorithme OU logique est appliqué).
- En l'absence d'entrée de correspondance, toutes les routes correspondent à la clause.
- Si une entrée d'ensemble n'est pas présente dans une clause d'autorisation de carte de routage, la route est redistribuée sans modification de ses attributs actuels.

Remarque Ne configurez pas d'entrée d'ensemble dans une clause de refus de carte de routage, car la clause de refus interdit la redistribution de routage : il n'y a aucun renseignement à modifier.

Une clause de carte de routage sans entrée de correspondance ou d'ensemble effectue une action. Une clause d'autorisation vide permet une redistribution des routes restantes sans modification. Une clause de refus vide ne permet pas une redistribution d'autres routes (il s'agit de l'action par défaut si une carte de routage est complètement analysée, mais qu'aucune correspondance explicite n'est trouvée).

Lignes directrices relatives aux cartes de routage

Mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Directives supplémentaires

Les cartes de routage ne prennent pas en charge les ACL qui incluent un utilisateur, un groupe d'utilisateurs ou des objets de nom de domaine complet.

Définir une carte de routage

Vous devez définir une carte de routage lorsque vous précisez les routes du protocole de routage spécifié qui peuvent être redistribuées dans le processus de routage cible. Dans ASDM, vous pouvez définir une carte de routage en ajoutant, en modifiant ou en supprimant un nom de carte de routage, un numéro de séquence ou une redistribution.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Route Maps (Cartes de routage)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add Route map** (Ajouter une carte de routage) ou **Edit Route Map** (Modifier une carte de routage) apparaît.

Étape 3 Saisissez le nom et le numéro de séquence de la carte de routage. Le nom de la carte de routage est le nom que vous attribuez à une route donnée. Le numéro de séquence est l'ordre dans lequel vous ajoutez ou supprimez les entrées de carte de routage dans l'ASA.

Remarque Si vous modifiez une carte de routage existante, les champs du nom et du numéro de séquence de la carte de routage sont déjà remplis.

Étape 4 Pour refuser les correspondances de routes de la redistribution, cliquez sur **Deny** (Refuser). Si vous utilisez une ACL dans une clause de refus de carte de routage, les routes autorisées par l'ACL ne sont pas redistribuées. Pour autoriser les correspondances de routes pour la redistribution, cliquez sur **Allow** (Autoriser). Si vous utilisez une ACL dans une clause d'autorisation de carte de routage, les routes autorisées par l'ACL sont redistribuées.

En outre, si vous utilisez une ACL dans une clause d'autorisation ou de refus de carte de routage et que l'ACL refuse une route, la correspondance de clause de carte de routage est introuvable et la clause de carte de routage suivante est évaluée.

Étape 5 Cliquez sur l'onglet **Match Clause** (Clause de correspondance) pour choisir les routes auxquelles cette clause doit être appliquée et définissez les paramètres suivants :

- Cochez la case **Match first hop interface of route** (Correspondance avec l'interface de premier saut de route) pour activer ou désactiver la correspondance avec l'interface de premier saut d'une route ou pour faire correspondre n'importe quelle route avec l'interface de saut suivant spécifiée. Si vous spécifiez plusieurs interfaces, la route peut correspondre à l'une ou l'autre des interfaces.
  - Saisissez le nom de l'interface dans le champ Interface ou cliquez sur les points de suspension pour afficher la boîte de dialogue Browse Interface (Parcourir l'interface).
  - Choisissez une ou plusieurs interfaces, cliquez sur **Interface**, puis cliquez sur **OK**.
- Dans les sections IPv4 et IPv6, effectuez une ou plusieurs des opérations suivantes :
  - Cochez la case **Match Address** (Correspondance d'adresse) pour activer ou désactiver la correspondance d'adresse d'une route ou d'un paquet de correspondance.
  - Cochez la case **Match Next Hop** (Correspondance de saut suivant) pour activer ou désactiver la correspondance d'adresse de saut suivant d'une route.
  - Cochez la case **Match Route Source** (Correspondance de source de route) pour activer ou désactiver la correspondance d'adresse de source d'annonce de la route.
  - Choisissez **Access List to Prefix List** (Liste d'accès à la liste de préfixes) dans la liste déroulante pour faire correspondre l'adresse IP.
  - Selon la sélection précédente, cliquez sur les points de suspension pour afficher la boîte de dialogue **Browse Access List** (Parcourir la liste d'accès) ou **Browse Prefix List** (Parcourir la liste de préfixes).
  - Choisissez l'ACL ou la liste de préfixes que vous souhaitez.
- Cochez la case **Match metric of route** (Correspondance de la mesure de la route) pour activer ou désactiver la correspondance de la mesure d'une route.
  - Dans le champ **Metric Value** (Valeur de mesure), saisissez les valeurs de la mesure. Il est possible d'entrer plusieurs valeurs, séparées par des virgules. Ce paramètre vous permet de faire correspondre toutes les routes qui ont une métrique spécifiée. La valeur de mesure peut être comprise entre 0 et 4294967295.
- Cochez la case **Match Route Type** (Correspondance du type de route) pour activer ou désactiver la correspondance du type de route. Les types de routage valides sont External1, External2, Internal, Local, NSSA-External1 et NSSA-External2. Lorsque cette option est activée, vous pouvez choisir plusieurs types de route dans la liste.

Étape 6 Cliquez sur l'onglet **Set Clause** (Définir la clause) pour modifier les renseignements suivants, qui seront redistribués au protocole cible :

- Cochez la case **Set Metric Clause** (Définir la clause de mesure) pour activer ou désactiver la valeur de mesure pour le protocole de routage de destination, et saisissez la valeur dans le champ Value (Valeur).
- Cochez la case **Set Metric Type** (Définir le type de mesure) pour activer ou désactiver le type de mesure pour le protocole de routage de destination, et choisissez le type de mesure dans la liste déroulante.
- **Adaptive Interface Metric Type** (Type de mesure de l'interface adaptative) : cette option se rapporte au routage basé sur des politiques. Cette option définit l'interface de sortie en fonction des valeurs de mesure recueillies sur les interfaces, à savoir le coût, le temps aller-retour (RTT), la gigue, la note d'opinion moyenne (MOS) et la perte (perte de paquets).
- Cliquez dans le champ **Available Interfaces** (Interfaces disponibles) et sélectionnez les interfaces qui doivent être utilisées pour le routage. L'interface de sortie est sélectionnée dans la liste des interfaces. Si les coûts des interfaces sont les mêmes, il s'agit d'une configuration active-active et les paquets sont équilibrés (round robin) sur les interfaces de sortie. Si les coûts sont différents, l'interface avec le coût le plus faible est sélectionnée. À l'instar de la mesure du coût, les autres valeurs sont appliquées en fonction du type de mesure, de la gigue minimale, du RTT minimal, de la perte de paquets minimale et de la MOS maximale. Les interfaces ne sont prises en compte que si elles sont actives.

Étape 7 Cliquez sur l'onglet BGP Match Clause (Clause de correspondance BGP) pour choisir les routes auxquelles cette clause doit être appliquée et définissez les paramètres suivants :

- Cochez la case **Match AS path access lists** (Correspondance des listes d'accès au chemin AS) pour permettre la mise en correspondance de la liste d'accès du système autonome BGP avec la liste d'accès au chemin spécifiée. Si vous spécifiez plusieurs listes d'accès de chemin d'accès, la voie de routage peut correspondre à l'une ou l'autre des listes d'accès de chemin d'accès.
- Cochez la case **Match Community** (Correspondance avec la communauté) pour activer la mise en correspondance de la communauté BGP avec la communauté spécifiée. Si vous spécifiez plusieurs communautés, la route peut correspondre à l'une ou à l'autre. Tout routage qui ne correspond pas à au moins une communauté de correspondance ne sera pas annoncée pour les cartes de routage sortantes.
  - Cochez la case Match the specified community exactly (Correspondance exacte avec la communauté spécifiée) pour activer la correspondance exacte entre la communauté de BGP et la communauté spécifiée.
- Cochez la case **Match Policy list** (Correspondance avec la liste de politiques) pour configurer une carte de routage afin d'évaluer et de traiter une politique de BGP. Si vous spécifiez plusieurs listes de politiques, la route peut traiter l'une ou l'autre de ces listes de politiques.

Étape 8 Cliquez sur l'onglet **BGP Set Clause** (Définir la clause de BGP) pour modifier les renseignements suivants, qui seront redistribués au protocole BGP :

- Cochez la case **Set AS Path** (Définir le chemin AS) pour modifier un chemin de système autonome pour les routes BGP.
  - Cochez la case Prepend AS path (Ajouter le chemin AS) pour ajouter une chaîne de chemin d'accès du système autonome quelconque aux routes BGP. Habituellement, le numéro du système autonome local est ajouté plusieurs fois, ce qui augmente la longueur du chemin du système autonome. Si vous spécifiez plusieurs numéros de chemin de système autonome, la route peut précéder l'un ou l'autre de ces numéros AS.

- Cochez la case Prepend Last AS to the AS Path (Ajouter le dernier AS au chemin AS) pour ajouter le dernier numéro AS au chemin. Saisissez une valeur pour le numéro de système autonome comprise entre 1 et 10.
- Cochez la case Convert route tag into AS Path (Convertir la balise de route en chemin AS) pour convertir la balise d'une route en chemin de système autonome.

- Cochez la **case Set Community** (Définir la communauté) **pour définir les attributs des communautés BGP.**
  - Cliquez sur le bouton radio Specify Community (Spécifier la communauté) pour saisir un numéro de communauté, le cas échéant. Les valeurs valides sont de 1 à 4294967200, internet, no-advertise et no-export.
  - Cochez la case Add to the existing communities (Ajouter aux communautés existantes) pour ajouter la communauté aux communautés déjà existantes.
  - Cliquez sur None (Aucun) pour supprimer l'attribut de communauté des préfixes qui transmettent la carte de routage.
- Cochez la case **Set local preference** (Définir la préférence locale) pour spécifier une valeur de préférence pour le chemin d'accès au système autonome.
- Cochez la case Set weight (Définir le poids) pour spécifier le poids du BGP pour la table de routage. Saisissez une valeur entre 0 et 65 535.
- Cochez la case Set origin (Définir l'origine) pour spécifier le code d'origine du BGP. Les valeurs valides sont Local IGP (IGP local) et Incomplete (Incomplet).
- Cochez la case Set next hop (Définir le saut suivant) pour préciser l'adresse de sortie des paquets qui répondent à la clause de correspondance d'une carte de routage.
  - Cliquez sur Specify IP address (Spécifier l'adresse IP) pour saisir l'adresse IP du prochain saut vers lequel les paquets sont sortis. Il n'est pas nécessaire qu'il s'agisse d'un routeur adjacent. Si vous spécifiez plusieurs adresses IP, les paquets peuvent être sortis à l'une ou l'autre des adresses IP.
  - Cliquez sur Use peer address (Utiliser l'adresse homologue) pour définir le saut suivant comme adresse homologue BGP.

Étape 9 Cliquez sur OK.

Personnaliser une carte de routage

Cette section décrit comment personnaliser la carte de routage.

Définir une route pour correspondre à une adresse de destination spécifique

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Route Maps (Cartes de routage)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue**Add Route map** (Ajouter une carte de routage) apparaît. Dans cette boîte de dialogue, vous pouvez attribuer ou choisir le nom de la carte de routage, le numéro de séquence et son accès de redistribution (c'est-à-dire autoriser ou refuser). Les entrées de carte de routage sont lues dans l'ordre. Vous pouvez identifier l'ordre à l'aide du numéro de séquence, ou l'ASA utilise l'ordre dans lequel vous ajoutez les entrées.

Étape 3 Cliquez sur l'onglet **Match Clause** (Clause de correspondance) pour choisir les routes auxquelles cette clause doit être appliquée et définissez les paramètres suivants :

- Cochez la case **Match first hop interface of route** (Correspondance avec l'interface de premier saut de route) pour activer ou désactiver la correspondance avec l'interface de premier saut d'une route ou pour faire correspondre n'importe quelle route avec l'interface de saut suivant spécifiée. Si vous spécifiez plusieurs interfaces, la route peut correspondre à l'une ou l'autre des interfaces.
  - Saisissez le nom de l'interface dans le champ **Interface** ou cliquez sur les points de suspension pour afficher la boîte de dialogue **Browse Interface** (Parcourir l'interface).
  - Choisissez le type d'interface (**interne** ou **externe**), cliquez sur **Selected Interface** (Interface sélectionnée), puis cliquez sur **OK**.
  - Cochez la case **Match IP Address** (Correspondance d'adresse IP) pour activer ou désactiver la correspondance d'adresse d'une route ou d'un paquet de correspondance.
  - Cochez la case **Match Next Hop** (Correspondance de saut suivant) pour activer ou désactiver la correspondance d'adresse de saut suivant d'une route.
  - Cochez la case **Match Route Source** (Correspondance de source de route) pour activer ou désactiver la correspondance d'adresse de source d'annonce de la route.
  - Choisissez **Access List to Prefix List** (Liste d'accès à la liste de préfixes) dans la liste déroulante pour faire correspondre l'adresse IP.
  - Selon la sélection précédente, cliquez sur les points de suspension pour afficher la boîte de dialogue **Browse Access List** (Parcourir la liste d'accès) ou **Browse Prefix List** (Parcourir la liste de préfixes).
  - Choisissez l'ACL ou la liste de préfixes que vous souhaitez.
- Cochez la case **Match metric of route** (Correspondance de la mesure de la route) pour activer ou désactiver la correspondance de la mesure d'une route.
  - Dans le champ **Metric Value** (Valeur de mesure), saisissez les valeurs de la mesure. Il est possible d'entrer plusieurs valeurs, séparées par des virgules. Ce paramètre vous permet de faire correspondre toutes les routes qui ont une métrique spécifiée. La valeur de mesure peut être comprise entre 0 et 4294967295.

- Cochez la case **Match Route Type** (Correspondance du type de route) pour activer ou désactiver la correspondance du type de route. Les types de routage valides sont External1, External2, Internal, Local, NSSA-External1 et NSSA-External2. Lorsque cette option est activée, vous pouvez choisir plusieurs types de route dans la liste.

Configurer les règles de préfixe



Remarque Vous devez configurer une liste de préfixes avant de pouvoir configurer une règle de préfixe.

Pour configurer des règles de préfixe, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **IPv4 Prefix Rules (Règles de préfixes IPv4)** ou **IPv6 Prefix Rules (Règles de préfixes IPv6)**.

Étape 2 Cliquez sur **Add** (Ajouter) et sélectionnez Add Prefix Rule (Ajouter une règle de préfixe).

La boîte de dialogue **Add Prefix Rule** (Ajouter une règle de préfixe) apparaît. Dans cette boîte de dialogue, vous pouvez ajouter un numéro de séquence, sélectionner une version IPv4 ou IPv6, spécifier un préfixe pour le réseau, son accès à la redistribution (c'est-à-dire autoriser ou refuser) et la longueur minimum et maximum du préfixe.

Étape 3 Saisissez un **Sequence Number** (Numéro de séquence) facultatif ou acceptez la valeur par défaut.

Étape 4 Spécifiez le **Prefix number** (Numéro de préfixe) au format adresse IP/longueur du masque.

Étape 5 Cliquez sur le bouton radio **Permit** (Autoriser) ou **Deny** (Refuser) pour indiquer l'accès à la redistribution.

Étape 6 Saisissez l'option **Minimum length** (Durée minimum) et **Maximum length** (Longueur maximum).

Étape 7 Cliquez sur **OK** lorsque vous avez terminé.

La nouvelle règle de préfixe ou la règle de préfixe révisée apparaît dans la liste.

Étape 8 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer les listes de préfixe

Lorsque plusieurs entrées d'une liste de préfixes correspondent à un préfixe donné, l'entrée avec le numéro de séquence le plus faible est utilisée. Par souci d'efficacité, vous pouvez placer les correspondances ou les refus les plus courants près du haut de la liste en leur attribuant manuellement un numéro de séquence inférieur. Par défaut, les numéros de séquence sont générés automatiquement par incréments de 5, en commençant par 5.

Pour ajouter des listes de préfixes, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **IPv4 Prefix Rules (Règles de préfixes IPv4)** ou **IPv6 Prefix Rules (Règles de préfixes IPv6)**.

Étape 2 Cliquez sur **Add (Ajouter)** > **Add Prefix List (Ajouter une liste de préfixes)**.

La boîte de dialogue **Add Prefix List** (Ajouter une liste de préfixes) s'affiche.

Étape 3 Saisissez le nom du préfixe et la description, puis cliquez sur **OK**.

Configurer les valeurs de mesure pour une action de routage

Pour configurer la valeur de mesure d'une action de routage, procédez comme suit :

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Route Maps (Cartes de routage)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add Route map** (Ajouter une carte de routage) ou **Edit Route Map** (Modifier une carte de routage) apparaît. Dans cette boîte de dialogue, vous pouvez attribuer ou sélectionner le nom de la carte de routage, le numéro de séquence et son accès de redistribution (c'est-à-dire autoriser ou refuser). Les entrées de carte de routage sont lues dans l'ordre. Vous pouvez identifier l'ordre à l'aide du numéro de séquence, ou l'ASA utilise l'ordre dans lequel vous ajoutez les entrées de la carte de routage.

Étape 3 Cliquez sur l'onglet **Set Clause** (Définir la clause) pour modifier les renseignements suivants, qui seront redistribués au protocole cible :

- Cochez la case **Set Metric Clause** (Définir la clause de mesure) pour activer ou désactiver la valeur de mesure pour le protocole de routage de destination, et entrez la valeur dans le champ Value (Valeur).
- Cochez la case **Set Metric Type** (Définir le type de mesure) pour activer ou désactiver le type de mesure pour le protocole de routage de destination, et choisissez le type de mesure dans la liste déroulante.

Exemple de cartes de routage

L'exemple suivant montre comment redistribuer les routes avec un nombre de sauts égal à 1 dans OSPF.

1. Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Route Maps (Cartes de routage)**.
2. Cliquez sur **Add** (ajouter).

3. Saisissez de **1 à 2** dans le champ **Route Map Name** (Nom de la carte de routage).
4. Saisissez le numéro de séquence de routage dans le champ **Séquence Number** (Numéro de séquence).
5. Cliquez sur le bouton radio **Permit** (Autoriser).

   Par défaut, cet onglet se trouve en haut.
6. Cliquez sur l'onglet **Match Clause** (Clause de correspondance).
7. Cochez la case **Match Metric of Route** (Correspondance métrique de la route) et saisissez **1** pour la valeur de la mesure.
8. Cliquez sur l'onglet **Set Clause** (Définir la clause).
9. Cochez la case **Set Metric Value** (Définir la valeur de mesure) et saisissez **5** comme valeur de mesure.
10. Cochez la case **Set Metric-Type** (Définir le type de mesure) et choisissez **Type-1**.

Historique des cartes de routage

Tableau 39 : Historique des fonctionnalités pour les cartes de routage

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Cartes de routage	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage).
Prise en charge améliorée pour les cartes de routage statiques et dynamiques	8.0(2)	Une prise en charge améliorée des cartes de routage dynamiques et statiques a été ajoutée.
Routage dynamique en mode de contexte multiple	9.0(1)	Les cartes de routage sont prises en charge en mode de contexte multiple.
Prise en charge BGP	9.2(1)	Nous avons introduit cette fonctionnalité. Nous avons mis à jour l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage) avec 2 onglets supplémentaires, BGP match clause (Clause de correspondance BGP) et BGP set clause (Clause de définition BGP).
Prise en charge d'IPv6 pour la règle de préfixe	9.3.2	Nous avons introduit cette fonctionnalité. Nous avons mis à jour les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **IPv4 Prefix Rules (Règles de préfixes IPv4)** et **IPv6 Prefix Rules (Règles de préfixes IPv6)**



CHAPITRE 32

Routage par détection de transfert bidirectionnel (BFD)

Ce chapitre décrit comment configurer l'ASA pour utiliser le protocole de routage par détection de transfert bidirectionnel (BFD).

- À propos du routage BFD, à la page 893
- Directives pour le routage BFD, à la page 896
- Configurer BFD, à la page 897
- Historique du routage BFD, à la page 900

À propos du routage BFD

BFD est un protocole de détection conçu pour fournir des temps de détection de défaillance du chemin d'acheminement rapides pour tous les types de médias, encapsulations, topologies et protocoles de routage. BFD fonctionne en mode point à point de monodiffusion en plus de tout protocole de données transféré entre deux systèmes. Les paquets sont transportés dans la charge utile du protocole d'encapsulation approprié pour le support et le réseau.

BFD fournit une méthode de détection des défaillances cohérente pour les administrateurs réseau en plus de la détection des défaillances du chemin de transfert rapide. Comme l'administrateur réseau peut utiliser BFD pour détecter les défaillances du chemin de transfert à un débit uniforme, plutôt que pour les débits variables, pour les différents mécanismes Hello du protocole de routage, le profilage et la planification du réseau sont plus faciles et le temps de reconversion est uniforme et prévisionnel.

Mode asynchrone BFD et fonction d'écho

La BFD peut fonctionner en mode asynchrone avec ou sans la fonction d'écho activée.

Mode asynchrone

En mode asynchrone, les systèmes envoient périodiquement des paquets de contrôle de la BFD l'un à l'autre, et si un certain nombre de paquets de la ligne ne sont pas reçus par l'autre système, la session est déclarée inactive. Le mode asynchrone pur (sans la fonction d'écho) est utile, car il nécessite deux fois moins de paquets pour atteindre un temps de détection particulier.

Fonction d'écho de la BFD

La fonction d'écho de la BFD envoie des paquets d'écho du moteur de transfert au voisin BFD à saut unique directement connecté. Les paquets écho sont envoyés par le moteur de transfert et redirigés le long du même chemin pour effectuer la détection. La session BFD à l'autre extrémité ne participe pas au transfert réel des paquets écho. Comme la fonction d'écho et le moteur de transfert sont responsables du processus de détection, le nombre de paquets de contrôle de la BFD qui sont envoyés entre les voisins de la BFD est réduit. Puisque le moteur de transfert teste le chemin de transfert sur le système voisin distant sans interagir avec le système distant, la variation du délai entre les paquets est augmentée. Cela se traduit par des délais de détection des défaillances plus rapides.

Lorsque la fonction d'écho est activée, la BFD peut utiliser la minuterie lente pour retarder la session asynchrone et réduire le nombre de paquets de contrôle de BFD envoyés entre les voisins de BFD, ce qui réduit le surdébit de traitement tout en permettant une détection plus rapide des défaillances.

Remarque La fonction d'écho n'est pas prise en charge pour les voisins BFD à multisaut IPv4 ou à saut unique IPv6.

Vous pouvez activer la BFD au niveau de l'interface et du protocole de routage. Vous devez configurer la BFD sur les deux systèmes (homologues BFD). Après avoir activé la BFD sur les interfaces et au niveau du routeur pour les protocoles de routage appropriés, une session BFD est créée, les minuteries de la BFD sont négociées et les homologues de la BFD commencent à s'envoyer des paquets de contrôle de la BFD au niveau négocié.

Établissement de la session BFD

L'exemple suivant montre l'ASA et un routeur voisin exécutant le protocole de passerelle frontière (BGP). Au moment où les deux appareils démarrent, aucune session BFD n'est établie entre eux.

Illustration 82 : Session BFD établie



Une fois que le protocole BGP a identifié son voisin BGP, il démarre le processus BFD avec l'adresse IP du voisin. La BFD ne détecte pas ses homologues de manière dynamique. Elle s'appuie sur les protocoles de routage configurés pour lui indiquer quelles adresses IP utiliser et quelles relations d'homologues former.

La BFD sur le routeur et la BFD sur l'ASA forment un paquet de contrôle de BFD et commencent à s'envoyer des paquets à un intervalle d'une seconde jusqu'à ce que la session BFD soit établie. Les paquets de contrôle initiaux de l'un ou l'autre des systèmes sont très similaires. Par exemple, les bits Vers, Diag, H, D, P et F sont tous définis sur zéro et l'état est défini sur Down (En panne). Le champ My Discriminator (Mon discriminateur) est défini sur une valeur unique sur le périphérique de transmission. Le champ Your Discriminator (Votre discriminateur) est défini sur zéro, car la session BFD n'a pas encore été établie. Les minuteries TX et RX sont définies aux valeurs trouvées dans la configuration de l'appareil.

Une fois que le périphérique BFD distant a reçu un paquet de contrôle de BFD pendant la phase d'ouverture de session, il copie la valeur du champ My Discriminator (Mon discriminateur) dans son propre champ Your Discriminator (Votre discriminateur) et la transition de l'état Down (En panne) à l'état Init (Initialisation), puis finalement à l'état Up (Opérationnel) se produit. Une fois que les deux systèmes ont vu leurs propres discriminateurs dans les paquets de contrôle de l'autre, la session est officiellement établie.

L'illustration suivante montre la connexion BFD établie.

Illustration 83 : BGP sans session BFD établie



Négociation de la minuterie BFD

Les appareils BFD doivent négocier les minuteries BFD pour contrôler et synchroniser le débit d'envoi des paquets de contrôle BFD. Un périphérique doit s'assurer des éléments suivants avant de pouvoir négocier une minuterie BFD :

- Que son appareil homologue a vu le paquet contenant les minuteries proposées par le périphérique local
- Qu'il n'envoie jamais de paquets de contrôle BFD plus rapidement que l'homologue n'est configuré pour les recevoir
- Que l'homologue n'envoie jamais de paquets de contrôle BFD plus rapidement que le système local n'est configuré pour les recevoir

Les paramètres du champ Your Discriminator (Votre discriminateur) et du bit H suffisent pour indiquer au périphérique local que le périphérique distant a vu ses paquets lors de l'échange initial de la minuterie. Après avoir reçu un paquet de contrôle BFD, chaque système prend l'intervalle RX minimum requis et le compare à son propre intervalle TX minimum souhaité, puis prend la plus grande (la plus lente) des deux valeurs et l'utilise comme débit de transmission pour ses paquets BFD. Le plus lent des deux systèmes détermine le débit de transmission.

Lorsque ces minuteries ont été négociées, elles peuvent être renégociées à tout moment pendant la session sans entraîner de réinitialisation de session. Le périphérique qui modifie ses minuteries règle le bit P sur tous les paquets de contrôle BFD suivants jusqu'à ce qu'il reçoive un paquet de contrôle BFD avec le bit F défini pour le système distant. Cet échange de bits permet d'éviter la perte de paquets pendant le transit.

Remarque Le réglage du bit F par le système distant ne signifie pas qu'il accepte les nouvelles minuteries proposées. Il indique que le système distant a vu les paquets dans lesquels les minuteries ont été modifiées.

Détection de défaillance BFD

Une fois la session BFD et les minuteries négociées, les homologues BFD s'envoient des paquets de contrôle BFD à l'intervalle négocié. Ces paquets de contrôle agissent comme une pulsation très similaire au protocole IGP Hello, sauf que le débit est plus accéléré.

Tant que chaque homologue de la BFD reçoit un paquet de contrôle de la BFD dans le cadre de l'intervalle de détection configuré (intervalle RX minimal requis), la session de la BFD reste active et tout protocole de routage associé à la BFD conserve ses contiguïtés. Si un homologue BFD ne reçoit pas de paquet de contrôle dans cet intervalle, il informe tous les clients participant à cette session BFD de la défaillance. Le protocole de routage détermine la réponse appropriée à ces renseignements. La réponse typique est de mettre fin à la session d'appairage du protocole de routage et de reconverger, et ainsi de contourner un homologue défaillant.

Chaque fois qu'un homologue BFD reçoit avec succès un paquet de contrôle BFD dans une session BFD, la minuterie de détection pour cette session est réinitialisée à zéro. La détection des défaillances dépend donc des paquets reçus et NON de la dernière transmission d'un paquet par le récepteur.

Scénarios de déploiement BFD

Les éléments suivants décrivent le fonctionnement de la BFD dans ces scénarios spécifiques.

Basculement

Dans un scénario de basculement, des sessions BFD sont établies et maintenues entre l'unité active et l'unité voisine. Les unités en veille ne maintiennent aucune session BFD avec leurs voisins. Lors d'un basculement, la nouvelle unité active doit initier l'établissement d'une session avec le voisin, car les renseignements sur la session ne sont pas synchronisés entre les unités actives et de secours.

Pour un scénario de redémarrage progressif/NSF, le client (BGP IPv4/IPv6) est chargé d'informer son voisin de l'événement. Lorsque le voisin reçoit les renseignements, il conserve la table RIB jusqu'à ce que le basculement soit terminé. Pendant le basculement, les sessions BFD et BGP sont inactives sur l'appareil. Une fois le basculement terminé, une nouvelle session BFD entre les voisins est établie lorsque la session BGP est lancée.

EtherChannel étendu et grappe L2

Dans un scénario de grappe EtherChannel étendu, la session BFD est établie et maintenue entre l'unité principale et son voisin. Les unités subordonnées ne maintiennent aucune session BFD avec leurs voisins. Si un paquet BFD est acheminé vers l'unité subordonnée en raison de l'équilibrage de charges sur le commutateur, l'unité subordonnée doit transférer ce paquet à l'unité principale par la liaison de grappe. Lorsqu'un basculement de grappe se produit, la nouvelle unité principale doit initier l'établissement d'une session avec le voisin, car les renseignements sur la session ne sont pas synchronisés entre les unités principale et subordonnée.

Mode d'interface individuelle et grappe L3

Dans un scénario de grappe en mode d'interface individuelle, les unités individuelles maintiennent leurs sessions BFD avec leurs voisins.

Directives pour le routage BFD

Directives relatives au mode contextuel

Pris en charge en modes de contexte unique et multiple.

Directives sur le mode pare-feu

Pris en charge en mode de pare-feu routé; prise en charge des modes autonome, de basculement et de grappe. La BFD n'est pas prise en charge sur les interfaces de basculement. Dans la mise en grappe, cette fonctionnalité n'est prise en charge que sur l'unité principale. La BFD n'est pas prise en charge en mode transparent.

Directives IPv6

Le mode Echo n'est pas pris en charge pour IPv6.

Directives supplémentaires

Les protocoles BGP IPv4et BGP IPv6 sont pris en charge.

Les protocoles OSPFv2, OSPFv3, IS-IS et EIGRP ne sont pas pris en charge.

La BFD pour les routes statiques n'est pas pris en charge.

La BFD de transfert et de tunnel n'est pas prise en charge.

Configurer BFD

Cette section décrit comment activer et configurer le processus de routage BFD sur votre système.

Procédure

Étape 1 Créer le modèle BFD, à la page 897.

Étape 2 Configurer les interfaces BFD, à la page 899.

Étape 3 Configurer les cartes BFD, à la page 899.

Créer le modèle BFD

Cette section décrit les étapes requises pour créer un modèle de BFD et passer en mode de configuration de la BFD.

Le modèle BFD spécifie un ensemble de valeurs d'intervalle BFD. Les valeurs d'intervalle BFD configurées dans le modèle BFD ne sont pas spécifiques à une interface unique. Vous pouvez également configurer l'authentification pour les sessions à saut unique et à sauts multiples. Vous pouvez activer Echo sur un seul saut uniquement.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BFD** > **Template (Modèle)**.

Étape 2 Cliquez sur **Add** ou **Edit** (Ajouter ou modifier) .

Utilisez la boîte de dialogue **Add BFD Template** (Ajouter un modèle de BFD) pour créer un nouveau modèle de BFD. Utilisez la boîte de dialogue **Edit BFD Template** (Modifier un modèle de BFD) pour modifier les paramètres existants.

Étape 3 Dans l'onglet **Template** (modèle), configurez les éléments suivants :

- **Template Name (**nom du modèle) : nom de ce modèle BFD. Vous devez attribuer un nom afin de configurer le reste des paramètres dans le modèle. Le nom du modèle ne peut pas avoir d'espaces.
- **Configuration Mode** (Mode de configuration) : sélectionnez **single-hop** (saut unique) ou **multi-hop** (multisaut) dans la liste déroulante.
- **Enable Echo** (activer Echo) : (facultatif) Active Echo pour le modèle à saut unique.

Si la fonction Echo n'est pas négociée, les paquets de contrôle BFD sont envoyés à un débit élevé pour respecter le temps de détection. Si la fonction Echo est négociée, les paquets de contrôle BFD sont envoyés à un débit négocié plus lent et les paquets d'écho autodirigés sont envoyés à un débit élevé. Nous vous conseillons d'utiliser le mode Echo si possible.

Étape 4 Dans l'onglet **Interval** (intervalle), configurez les éléments suivants :

a) Dans la liste déroulante **Interval Type** (Type d'intervalle), sélectionnez **None** (Aucun), **Both** (Les deux), **Microseconds** (Microsecondes) ou **Milliseconds** (Millisecondes).

b) Si vous avez sélectionné **Both** (Les deux), configurez les options suivantes :

- **Multiplier Values** (Valeurs de multiplicateur) : la valeur utilisée pour calculer le délai de rétention. Indique le nombre de paquets de contrôle BFD consécutifs qui doivent être manqués par un homologue BFD avant que la BFD ne déclare que l'homologue n'est pas disponible et que l'homologue BFD de couche 3 soit informé de la défaillance. La valeur doit être comprise entre 3 et 50. La valeur par défaut est de 3.
- **Both Transmit and Receive Values** (Valeurs de transmission et de réception) : la capacité minimale d'intervalle de transmission et de réception. La plage va de 50 à 999 millisecondes.

c) Si vous avez sélectionné **Microseconds** (Microseconds), vous pouvez cliquer sur le bouton radio **Both** (Les deux) et configurer les éléments suivants :

- **Multiplier Values** (Valeurs de multiplicateur) : la valeur utilisée pour calculer le délai de rétention. Indique le nombre de paquets de contrôle BFD consécutifs qui doivent être manqués par un homologue BFD avant que la BFD ne déclare que l'homologue n'est pas disponible et que l'homologue BFD de couche 3 soit informé de la défaillance. La valeur doit être comprise entre 3 et 50. La valeur par défaut est de 3.
- **Minimum Transmit Values** (Valeurs de transmission minimum) : l'intervalle de transmission minimum. La plage se situe entre 50 000 et 999 000 microsecondes.
- **Minimum Receive Values** (Valeurs de réception minimum) : l'intervalle de réception minimum. La plage se situe entre 50 000 et 999 000 microsecondes.

d) Si vous avez sélectionné **Milliseconds** (Millisecondes), configurez les éléments suivants :

- **Multiplier Values** (Valeurs de multiplicateur) : indique le nombre de paquets de contrôle BFD consécutifs qui doivent être manqués par un homologue BFD avant que la BFD ne déclare que l'homologue n'est pas disponible et que l'homologue BFD de couche 3 soit informé de la défaillance. La valeur doit être comprise entre 3 et 50.
- **Minimum Transmit Values** (Valeurs de transmission minimum) : l'intervalle de transmission minimum. La plage va de 50 à 999 millisecondes.
- **Minimum Receive Values** (Valeurs de réception minimum) : l'intervalle de réception minimum. La plage va de 50 à 999 millisecondes.

Étape 5 Sous l'onglet **Authentication** (authentification), configurez les éléments suivants :

- **Authentication Type** (Type d'authentification) : sélectionnez **NONE** (AUCUN), **md5**, **meticulous-sha-1**, **meticulous-md5** ou **sha-1** dans la liste déroulante.
- **Key Value** (Valeur de clé) : la châine d'authentification qui doit être envoyée et reçue dans les paquets utilisant le protocole de routage en cours d'authentification. La valeur valide est une chaîne contenant de 1 à 17 caractères alphanumériques majuscules et minuscules, sauf que le premier caractère NE PEUT PAS être un chiffre.
- **Key ID** : ID de clé partagée qui correspond à la valeur de clé.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Apply** (Appliquer) pour enregistrer la configuration du modèle BFD.

Configurer les interfaces BFD

Vous pouvez lier un modèle BFD à une interface, configurer les paramètres de session BFD de référence par interface et activer le mode écho par interface.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BFD** > **Interface**.

Étape 2 Cliquez sur **Add** ou **Edit**(ajouter ou modifier) .

Utilisez la boîte de dialogue **Add Interface** (Ajouter une interface) pour configurer une nouvelle interface BFD. Utilisez la boîte de dialogue **Edit Interface** (Modifier l'interface) pour modifier les paramètres existants.

Étape 3 Dans la liste déroulante **Interface**, sélectionnez l'interface que vous souhaitez configurer avec la BFD.

Étape 4 Cochez la case **Template Name** (Nom du modèle) et choisissez un modèle BFD dans la liste déroulante.

Étape 5 Configurez les intervalles BFD suivants :

- **Minimum Transmit Values** (Valeurs de transmission minimum) : l'intervalle de transmission minimum. La plage va de 50 à 999 millisecondes.
- **Minimum Receive Values** (Valeurs de réception minimum) : l'intervalle de réception minimum. La plage va de 50 à 999 millisecondes.
- **Multiplier** (Multiplicateur) : indique le nombre de paquets de contrôle BFD consécutifs qui doivent être manqués par un homologue BFD avant que la BFD ne déclare que l'homologue n'est pas disponible et que l'homologue BFD de couche 3 soit informé de la défaillance. La valeur doit être comprise entre 3 et 50.

Étape 6 (Facultatif) Cochez la case **Echo** (Écho) si vous souhaitez avoir le mode écho sur cette interface. Vous ne pouvez activer le mode écho que sur les modèles à saut unique.

Étape 7 Cliquez sur **OK**.

Configurer les cartes BFD

Vous pouvez créer une carte BFD contenant des destinations que vous pouvez associer à un modèle multisaut. Vous devez disposer d'un modèle BFD multisaut déjà configuré.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BFD** > **Map (Carte)**.

Étape 2 Cliquez sur **Add** ou **Edit** (ajouter ou modifier) .

Utilisez la boîte de dialogue **Add Map** (Ajouter une carte) pour configurer une nouvelle carte BFD. Utilisez la boîte de dialogue **Edit Map** (Modifier la carte) pour modifier les paramètres existants.

Étape 3 Dans la liste déroulante **Template Name** (Nom du modèle), sélectionnez un modèle BFD.

Étape 4 Configurez les intervalles BFD suivants :

- **Minimum Transmit Values** (Valeurs de transmission minimum) : l'intervalle de transmission minimum. La plage va de 50 à 999 millisecondes.
- **Minimum Receive Values** (Valeurs de réception minimum) : l'intervalle de réception minimum. La plage va de 50 à 999 millisecondes.
- **Multiplier** (Multiplicateur) : indique le nombre de paquets de contrôle BFD consécutifs qui doivent être manqués par un homologue BFD avant que la BFD ne déclare que l'homologue n'est pas disponible et que l'homologue BFD de couche 3 soit informé de la défaillance. La valeur doit être comprise entre 3 et 50.

Étape 5 Cliquez sur **OK**.

Historique du routage BFD

Tableau 40 : Historique des fonctionnalités du routage BFD

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge du routage BFD	9.6(2)	L'ASA prend désormais en charge le protocole de routage BFD. Une prise en charge a été ajoutée pour la configuration des modèles, des interfaces et des cartes BFD. La prise en charge du protocole de routage BGP pour utiliser BFD a également été ajoutée. Nous avons ajouté ou modifié les écrans suivants : **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BFD > Template (Modèle)** **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BFD > Interface** **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BFD > Map (Carte)** **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > IPv6 Family (Famille IPv6) > Neighbor (Voisin)**



CHAPITRE 33

BGP

Ce chapitre décrit comment configurer l'ASA pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole de passerelle frontière (BGP).

- BGP, à la page 901
- Lignes directrices BGP, à la page 905
- Configurer le protocole BGP, à la page 906
- Supervision BGP, à la page 928
- Historique de BGP, à la page 929

BGP

Le protocole de passerelle frontière (BGP) est un protocole de routage inter et intra-systèmes autonomes qui

- fonctionne au sein des systèmes autonomes et entre ceux-ci (réseaux ou groupes de réseaux soumis à une administration et à des politiques de routage communes),
- échange des informations de routage pour Internet, et
- sert de protocole entre les fournisseurs de services Internet (FSI).

Scénarios d'utilisation de BGP

Les scénarios d'utilisation de BGP sont des configurations réseau qui

- permettent aux fournisseurs de services Internet d'échanger des routes client et ISP entre des systèmes autonomes à l'aide d'un BGP externe (EBGP),
- permettent aux fournisseurs de services d'échanger des routes au sein d'un système autonome utilisant le BGP intérieur (IBGP), et
- prennent en charge le routage de préfixe IPv6 sur les réseaux IPv6.

Contextes de mise en œuvre de BGP

Les réseaux des clients, comme les universitaires et les entreprises, emploient généralement un protocole IGP (Interior Gateway Protocol) comme OSPF pour l'échange d'informations de routage au sein de leurs réseaux. Les clients se connectent aux fournisseurs de services Internet, et les fournisseurs de services Internet utilisent

BGP pour échanger les routes du client et des fournisseurs de services Internet. Lorsque BGP est utilisé entre des systèmes autonomes (AS), le protocole est appelé BGP externe (EBGP). Si un fournisseur de services utilise BGP pour échanger des routages au sein d'un système autonome, le protocole est appelé BGP intérieur (IBGP).

BGP peut également être utilisé pour acheminer des informations de routage pour le préfixe IPv6 sur les réseaux IPv6.



Remarque Lorsqu'un périphérique BGPv6 rejoint la grappe, il génère un traçage logiciel lorsque le niveau de journalisation 7 est activé.

Modifications apportées à la table de routage

Les modifications de tableau de routage sont des mises à jour de réseau qui

- se produisent lorsque les voisins BGP échangent des informations de routage complètes lors de l'établissement initial de la connexion TCP
- impliquent l'envoi uniquement des routes modifiées aux voisins lorsque des modifications de table de routage sont détectées, et
- annoncent uniquement le CHEMIN optimal vers un réseau de destination sans mises à jour périodiques.

Attributs BGP pour la sélection de la voie de routage

Les voies de routage apprises via BGP ont des propriétés utilisées pour déterminer la meilleure voie de routage lorsque plusieurs chemins vers une destination existent. Ces propriétés sont appelées attributs BGP et sont utilisées dans le processus de sélection de la voie de routage :

- Pondération : il s'agit d'un attribut défini par Cisco qui est local à un routeur. L'attribut de pondération n'est pas annoncé aux routeurs voisins. Si le routeur détecte l'existence de plusieurs routes vers la même destination, la route ayant la pondération la plus élevée est préférée.
- Préférence locale : l'attribut de préférence locale est utilisé pour sélectionner un point de sortie du système autonome local. Contrairement à l'attribut de poids, il est partagé dans l'ensemble du système autonome local. S'il y a plusieurs points de sortie, celui dont l'attribut de préférence locale est le plus élevé est choisi pour une voie de routage spécifique.
- Identifiant multi-sortie : L'attribut de métrique ou de discrimination multi-sortie (MED) est utilisé comme suggestions à un système autonome externe concernant la voie de routage préférée dans le système autonome qui annonce la métrique. Il s'agit d'une suggestions, car le système autonome externe qui reçoit les MED peut également utiliser d'autres attributs de BGP pour la sélection de route. La route avec la métrique MED la plus basse est préférée.
- Origine : l'attribut d'origine indique comment BGP a appris l'existence d'une route particulière. L'attribut d'origine peut avoir l'une des trois valeurs possibles et est utilisé dans la sélection de la route.
  - IGP : la voie de routage est intérieure au système autonome d'origine. Cette valeur est définie lorsque la commande de configuration du routeur network est utilisée pour injecter la voie de routage dans BGP.
  - EGP : le routage est appris par le protocole EBGP (Exterior Border Gateway Protocol).

- Incomplet : l’origine de la route est inconnue ou apprise d’une autre manière. Une origine incomplète se produit lorsqu'une route est redistribuée dans BGP.

- AS_path : lorsqu’une déclaration de route passe par un système autonome, le numéro de système autonome est ajouté à une liste ordonnée de numéros de système autonome que l’annonce de route a traversés. Seule la voie de routage avec la liste AS_path la plus courte est installée dans la table de routage IP.
- Saut suivant : l'attribut de saut suivant EBGP est l'adresse IP utilisée pour atteindre le routeur publicitaire. Pour les homologues EBGP, l’adresse de saut suivant est l’adresse IP de la connexion entre les homologues. Pour IBGP, l’adresse du prochain saut EBGP est acheminée dans le système autonome local. Cependant, lorsque le saut suivant se trouve dans le même sous-réseau que l’adresse d’appairage de l’homologue eBGP, le saut suivant n’est pas modifié. Ce comportement est appelé saut suivant du tiers.

  Utilisez la commande **next-hop-self** lors de la redistribution des routes annoncées par VPN vers les homologues iBGP pour vous assurer que les routes sont redistribuées avec l’adresse IP du prochain saut appropriée.
- Community (Communauté) : l’attribut Community permet de regrouper des destinations, appelées communautés, auxquelles les décisions de routage (telles que l’acceptation, les préférences et la redistribution) peuvent être appliquées. Des cartes de routage sont utilisées pour définir l’attribut de communauté. Les attributs de communauté prédéfinis sont les suivants :
  - no-export : n’annonce pas cette voie de routage aux homologues EBGP.
  - no-advertise : n’annonce cette voie de routage à aucun homologue.
  - Internet : annonce cette route à la communauté Internet; tous les routeurs du réseau lui appartiennent.



Remarque La détection de boucle AS se fait en analysant le chemin AS complet (comme spécifié dans l’attribut AS_PATH) et en vérifiant que le numéro de système autonome du système local ne figure pas dans le chemin AS. Par défaut, EBGP annonce les routes apprises au même homologue pour éviter des cycles de CPU supplémentaires sur la périphérique lors des vérifications de boucle et des retards dans les tâches de mise à jour sortantes existantes.

Sélection du chemin BGP

La sélection de chemin BGP est un processus de routage qui sélectionne un seul chemin comme meilleur chemin lorsque BGP reçoit plusieurs annonces pour la même voie de routage de différentes sources, place le chemin sélectionné dans la table de routage IP et propage le chemin à ses voisins à l’aide de critères spécifiques dans l’ordre de priorité.

Critères de sélection du chemin BGP

BGP utilise les critères suivants, dans l’ordre présenté, pour sélectionner un chemin pour une destination :

1. Si le chemin précise un saut suivant inaccessible, supprimez la mise à jour. Privilégiez le chemin avec la pondération la plus élevée.

2. Si les pondérations sont identiques, préférez le chemin avec la préférence locale la plus élevée. Si les préférences locales sont les mêmes, le chemin préféré est celui qui a été créé par le protocole BGP exécuté sur ce routeur.
3. Si aucune voie de routage n'a été créée, privilégiez la voie de routage qui a le chemin AS_path le plus court. Si tous les chemins ont la même longueur AS_path, privilégiez le chemin avec le type d'origine le plus bas (où IGP est inférieur à EGP et EGP est inférieur à incomplet).
4. Si les codes d'origine sont les mêmes, privilégiez le chemin avec l'attribut MED le plus bas. Si les chemins ont la même MED, privilégiez le chemin externe au chemin interne.
5. Si les chemins sont toujours les mêmes, privilégiez le chemin par le voisin IGP le plus proche. Déterminez si plusieurs chemins d'accès nécessitent l'installation dans la table de routage pour Chemins multiples BGP, à la page 904.
6. Déterminez si plusieurs chemins d'accès nécessitent l'installation dans la table de routage pour Chemins multiples BGP, à la page 904.
7. Si les deux chemins sont externes, privilégiez le chemin qui a été reçu en premier (le plus ancien).
8. Privilégiez le chemin avec l'adresse IP la plus basse, comme spécifié par l'ID du routeur BGP. Si l'ID de l'expéditeur ou du routeur est le même pour plusieurs chemins, privilégiez le chemin avec la longueur minimale de la liste de grappes.
9. Privilégiez le chemin qui provient de l'adresse du voisin le plus bas.

Chemins multiples BGP

Les chemins multiples BGP sont une fonctionnalité BGP qui

- permet l'installation dans la table de routage IP de plusieurs chemins BGP à coût égal vers le même préfixe de destination,
- permet de répartir le trafic vers le préfixe de destination sur tous les chemins installés, et
- n'affecte pas l'algorithme de sélection du meilleur chemin.

Exigences relatives aux chemins multiples BGP

Ces chemins sont installés dans le tableau avec le meilleur chemin pour le partage de la charge. Les chemins multiples BGP n'affectent pas la sélection du meilleur chemin. Par exemple, un routeur désigne toujours l'un des chemins comme le meilleur chemin, selon l'algorithme, et annonce ce meilleur chemin à ses homologues de BGP.

Pour être candidats aux chemins multiples, les chemins vers la même destination doivent présenter les mêmes caractéristiques que le meilleur chemin :

- Poids
- Préférence locale
- Longueur du chemin d'accès AS
- Code d'origine
- Sélecteur de sorties multiples (MED)

- L'une des suivantes :
  - Le système autonome ou sous-système autonome voisin (avant l'ajout des chemins multiples de BGP)
  - AS-PATH (après l'ajout des chemins multiples BGP)

Certaines fonctionnalités de chemins multiples BGP imposent des exigences supplémentaires aux chemins candidats :

- Le chemin doit être appris d'un voisin externe ou d'un voisin externe à la confédération (eBGP).
- La métrique IGP jusqu'au saut suivant BGP doit être égale à la métrique IGP du meilleur chemin.

Voici les exigences supplémentaires pour les candidats aux chemins multiples de BGP interne (iBGP) :

- Le chemin doit être appris d'un voisin interne (iBGP).
- La métrique IGP jusqu'au saut suivant BGP doit être égale à la métrique IGP du meilleur chemin, sauf si le routeur est configuré pour les chemins multiples iBGP à coût inégal.

BGP insère dans la table de routage IP jusqu'aux *n* chemins les plus récemment reçus parmi les chemins candidats, où *n* correspond au nombre de routes à installer dans la table de routage, comme indiqué lors de la configuration des chemins multiples BGP. La valeur par défaut, lorsque les chemins multiples est désactivé, est 1.

Pour l'équilibrage de charge à coût inégal, vous pouvez également utiliser la bande passante du lien BGP.

Remarque L'équivalent de next-hop-self est appliqué au meilleur chemin sélectionné parmi les chemins multiples eBGP avant son transfert aux homologues internes.

Lignes directrices BGP

Lignes directrices relatives au mode contextuel

Tenez compte de ces exigences en mode contexte lors de la mise en œuvre de BGP.

- Pris en charge en mode contexte unique et multiple.
- Un seul numéro du système autonome (AS) est pris en charge pour tous les contextes.

Lignes directrices sur le mode pare-feu

Le mode pare-feu transparent n'est pas pris en charge. BGP est pris en charge uniquement en mode routé.

Lignes directrices IPv6

Prend en charge IPv6.

Lignes directrices supplémentaires

Tenez compte de ces exigences et limites opérationnelles supplémentaires.

- Le système n'ajoute pas d'entrée de routage pour l'adresse IP reçue sur PPPoE dans la table de routage du CP. BGP recherche toujours dans la table de routage du CP le lancement de la session TCP. Par conséquent, BGP ne forme pas de session TCP.

  C'est pourquoi, BGP sur PPPoE n'est pas pris en charge.

- BGP n’est pas pris en charge sur les interfaces BVI ou de gestion uniquement.
- Pour éviter les oscillations de contiguïté dues aux mises à jour de routage abandonnées si la mise à jour de routage est supérieure à la MTU minimale sur le lien, configurez la même MTU sur les interfaces des deux côtés du lien.
- BGP avec PATH MTU (PMTU) peut entraîner des fluctuations de contiguïté en cas d’échec de la découverte de la MTU, en particulier avec le routage ECMP. Par conséquent, soyez prudent lorsque vous utilisez BGP, PMTU et ECMP, car des abandons de paquets peuvent se produire si la découverte de la MTU échoue pour une raison quelconque.
- La table BGP de l’unité membre n’est pas synchronisée avec la table de l’unité de contrôle. Seule sa table de routage est synchronisée avec celle de l’unité de contrôle.
- Activez la fonctionnalité de délai d’expiration progressif lorsque vous utilisez BGP sur les périphériques Firewall Threat Defense configurés en mode de haute accessibilité. L’activation de cette fonctionnalité réduit les abandons de paquets qui se produisent en raison de problèmes liés à la convergence de BGP.

Configurer le protocole BGP

Cette section décrit comment activer et configurer le processus BGP sur votre système.

Procédure

Étape 1 Activer BGP, à la page 906.
Étape 2 Définir le meilleur chemin pour un processus de routage BGP, à la page 908.
Étape 3 Configurer les listes de politiques, à la page 909.
Étape 4 Configurer les filtres de chemin AS, à la page 910.
Étape 5 Configurer les règles de communauté, à la page 911.
Étape 6 Configurer les paramètres de la famille d’adresses IPv4, à la page 912.
Étape 7 Configurer les paramètres de la famille d’adresses IPv6, à la page 920.

Activer BGP

Cette section décrit les étapes requises pour activer le routage BGP, établir un processus de routage BGP et configurer les paramètres BGP généraux.

Procédure

Étape 1 Pour le mode unique, dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **General (Général)**.



Remarque Pour le multimode, dans ASDM, choisissez Configuration > Context Management (Gestion de contextes) > BGP. Après avoir activé BGP, passez à un contexte de sécurité et activez BGP en choisissant **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > General (Général)**.

Étape 2 Cochez la case **Enable BGP Routing** (Activer le routage BGP).

Étape 3 Dans le champ AS Number (numéro de système autonome), saisissez le numéro de système autonome (AS) pour le processus BGP. Le numéro de système autonome comprend plusieurs numéros autonomes en interne. Le numéro AS peut être compris entre 1 et 4294967295 ou entre 1.0 et XX.YY.

Étape 4 (Facultatif) Cochez la case **Limit the number of AS numbers in the AS_PATH attribute of received routes** (Limiter le nombre de numéros du système autonome dans l'attribut AS_PATH des routes reçues) pour restreindre le nombre de numéros du système autonome dans l'attribut AS_PATH à un nombre précis. Les valeurs valides sont comprises entre 1 et 254.

Étape 5 (Facultatif) Cochez la case Log neighbor changes (Consigner les modifications des voisins) pour activer la journalisation des modifications du voisin de BGP (actives ou différées) et des réinitialisations. Cela aide à résoudre les problèmes de connectivité du réseau et à mesurer la stabilité du réseau.

Étape 6 (Facultatif) Cochez la case Use TCP path MTU discovery (Utiliser la découverte de la MTU de chemin TCP) pour utiliser la technique de découverte de la MTU du chemin afin de déterminer la taille maximale de l'unité de transmission (MTU) sur le chemin réseau entre deux hôtes IP. Cela permet d'éviter la fragmentation IP.

Étape 7 (Facultatif) Cochez la case Enable fast external failover (Activer le basculement externe rapide) pour réinitialiser la session de BGP externe immédiatement en cas de défaillance de la liaison.

Étape 8 (Facultatif) Cochez la case Enforce that first AS is peer's AS for EBGP Routes (Veiller à ce que le premier AS soit l'AS de l'homologue pour les routes EBGP) pour ignorer les mises à jour entrantes reçues d'homologues de BGP externes qui n'indiquent pas leur numéro de système autonome comme premier segment dans l'attribut AS_PATH. Cela empêche un homologue mal configuré ou non autorisé d'acheminer le trafic en affichant un routage comme s'il provenait d'un autre système autonome.

Étape 9 (Facultatif) Cochez la case Use dot notation for AS numbers (Utiliser la notation par point pour les numéros d'AS) afin de scinder le numéro AS complet de 4 octets binaires en deux mots de 16 bits chacun, séparés par un point. Les numéros AS de 0 à 65 553 sont représentés sous forme de nombres décimaux et les nombres AS supérieurs à 65 535 sont représentés à l'aide de la notation par point.

Étape 10 Fournissez les renseignements sur la minuterie dans la zone Neighbor timers (Minuteries de voisin) :

a) Dans le champ Keepalive interval (Intervalle Keepalive), saisissez l'intervalle de temps pendant lequel le voisin de BGP reste actif après n'avoir pas envoyé de message keepalive. À la fin de cet intervalle de maintien, l'homologue de BGP est déclaré mort si aucun message n'est envoyé. La valeur par défaut est 60 secondes.

b) Dans le champ Hold Time (Délai de rétention), saisissez l'intervalle de temps pendant lequel le voisin de BGP reste actif pendant qu'une connexion BGP est lancée et configurée. Les valeurs par défaut sont de 180 secondes.

c) (Facultatif) Dans le champ Min. Hold Time (Délai de rétention min.), saisissez l'intervalle de temps minimal pendant lequel le voisin de BGP reste actif pendant qu'une connexion BGP est lancée et configurée. Spécifiez une valeur comprise entre 0 et 65 535.



Remarque Une durée d'attente de moins de 20 secondes augmente les risques d'intermittence des pairs

Étape 11 (Facultatif) Dans la section Non Stop Forwarding (Transfert continu), procédez comme suit :

a) Cochez la case Enable Graceful Restart (Activer le redémarrage progressif) pour permettre aux homologues de l'ASA d'éviter une oscillation de routage à la suite d'un basculement.

b) Dans le champ Restart Time (Heure de redémarrage), précisez la durée pendant laquelle les homologues de l'ASA attendront pour supprimer les routes périmées avant qu'un message d'ouverture de BGP ne soit reçu. La valeur par défaut est 120secondes. Les valeurs valides sont comprises entre 1 et 3600.

c) Dans le champ Stale Path Time (Temps de parcours), saisissez la durée pendant laquelle l'ASA attendra avant de supprimer des routes périmées après la réception d'un message de fin d'enregistrement (EOR) de la part de l'ASA, qui redémarrera. La valeur par défaut est 360 secondes. Les valeurs valides sont comprises entre 1 et 3600.

Étape 12 Cliquez sur **OK**.

Étape 13 Cliquez sur **Apply** (Appliquer).

Définir le meilleur chemin pour un processus de routage BGP

Cette section décrit les étapes requises pour configurer le meilleur chemin BGP. Pour en savoir plus sur le meilleur chemin, consultez Sélection du chemin BGP, à la page 903.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **Best Path (Meilleur chemin)**.

Le volet de configuration Best Path (Meilleur chemin) apparaît.

Étape 2 Dans le champ Default Local Preference (Préférence locale par défaut) spécifiez une valeur comprise entre 0 et 4294967295. La valeur par défaut est 100. Des valeurs plus élevées indiquent une préférence plus élevée. Cette préférence est envoyée à tous les routeurs et serveurs d'accès du système autonome local.

Étape 3 Cochez la case Allow comparing MED from different neighbors (Permet de comparer les MED de différents voisins) pour autoriser la comparaison du Discriminateur multi-sortie (MED) pour les chemins de voisins dans différents systèmes autonomes.

Étape 4 Cochez la case Compare router-id for identical EBGP paths (Comparer l'ID du routeur pour des chemins EBGP identiques) pour comparer les chemins similaires reçus d'homologues externes de BGP pendant le processus de sélection du meilleur chemin et faire passer le meilleur chemin à la route ayant le plus petit ID de routeur.

Étape 5 Cochez la case Pick the best MED path among paths advertised from the neighboring AS (Choisir le meilleur chemin MED parmi les chemins annoncés par l'AS voisin) pour activer la comparaison MED parmi les

chemins appris des homologues de la confédération. Ajoutez une nouvelle entrée réseau. La comparaison entre les MED est effectuée uniquement s'il n'y a aucun système autonome externe sur le chemin.

Étape 6 Cochez la case Treat missing MED as the least preferred one (Traiter le MED manquant comme le moins préféré) pour considérer l'attribut MED manquant comme ayant une valeur infinie, faisant de ce chemin le moins souhaitable; par conséquent, un chemin pour lequel un MED manquant est défaillant est préférable.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur Apply (appliquer).

Configurer les listes de politiques

Lorsqu'une liste de stratégie est référencée dans une carte de routage, toutes les déclarations de correspondance dans la liste de stratégie sont évaluées et traitées. Deux listes de politiques ou plus peuvent être configurées avec une carte de routage. Une liste de politiques peut également coexister avec d'autres instructions de mise en correspondance et d'ensemble préexistantes configurées dans la même carte de routage, mais en dehors de la liste de politiques. Cette section décrit les étapes requises pour configurer les listes de politiques.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **Policy Lists (Listes de politiques)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue Add Policy List (Ajouter une liste de politiques) s'affiche. À partir de cette boîte de dialogue, vous pouvez ajouter un nom de liste de politiques, son accès à la redistribution (c'est-à-dire autoriser ou refuser), faire correspondre des interfaces, spécifier des adresses IP, faire correspondre le chemin AS, faire correspondre la liste des noms de communauté, faire correspondre les mesures et faire correspondre les numéros de balise.

Étape 3 Dans le champ **Policy List Name**(Nom de la liste de politiques), entrez un nom unique pour la liste de politiques.

Étape 4 Cliquez sur le bouton radio **Permit** (Autoriser) ou **Deny** (Refuser) pour indiquer l'accès à la redistribution.

Étape 5 Cochez la case **Match Interfaces** (Correspondance des interfaces) pour distribuer les routes dont le prochain saut se trouve hors de l'une des interfaces spécifiées, puis effectuez l'une des opérations suivantes :

- Dans le champ **Interface**, saisissez le nom de l'interface.
- Dans le champ Interface, cliquez sur les points de suspension pour rechercher manuellement et localiser l'interface. Choisissez une ou plusieurs interfaces, cliquez sur **Interface**, puis cliquez sur **OK**.

Étape 6 Dans la zone Specify IP (Spécifier l'adresse IP), configurez les éléments suivants :

a) Cochez la case Match Address (Correspondance des adresses) pour redistribuer toutes les routes dont l'adresse réseau de destination est autorisée par une liste d'accès standard ou une liste de préfixes, et effectuez le routage des politiques sur les paquets.

Spécifiez une liste d'accès ou une liste de préfixes ou cliquez sur les points de suspension pour rechercher manuellement et localiser une liste d'accès. Choisissez une ou plusieurs listes d'accès, cliquez sur Access List (Liste d'accès), puis cliquez sur OK.

b) Cochez la case Match Next Hop (Correspondance des sauts suivants) pour redistribuer toutes les routes dont l'adresse du routeur de saut suivant est transmise par l'une des listes d'accès ou listes de préfixes spécifiées.

Spécifiez une liste d'accès/liste de préfixes ou cliquez sur les points de suspension pour rechercher manuellement et localiser une liste d'accès. Choisissez une ou plusieurs listes d'accès, cliquez sur Access List (Liste d'accès), puis cliquez sur OK.

c) Cochez la case Match Route Source (Correspondance source de route) pour redistribuer les routes qui ont été annoncées par les routeurs et les serveurs d'accès à l'adresse spécifiée par les listes d'accès ou la liste de préfixes.

Spécifiez une liste d'accès/liste de préfixes ou cliquez sur les points de suspension pour rechercher manuellement et localiser une liste d'accès. Choisissez une ou plusieurs listes d'accès, cliquez sur Access List (Liste d'accès), puis cliquez sur OK.

Étape 7 Cochez la case Match AS Path (Correspondance du chemin AS) pour faire correspondre un chemin de système autonome BGP.

Spécifiez un filtre de chemin AS ou cliquez sur les points de suspension pour rechercher manuellement et localiser le filtre de chemin AS. Choisissez un ou plusieurs filtres de chemin AS, cliquez sur AS Path Filter (Filtre de chemin AS), puis sur OK.

Étape 8 Cochez la case Match Community Names List (Associer la liste de noms de communauté) pour faire correspondre une communauté BGP.

a) Spécifiez une règle de communauté ou cliquez sur les points de suspension pour rechercher manuellement et localiser les règles de communauté. Sélectionnez une ou plusieurs règles de communauté, cliquez sur Community Rules (Règles de communauté), puis sur OK.
b) Cochez la case Match the specified community exactly (Faire correspondre exactement la communauté spécifiée) pour faire correspondre une communauté BGP spécifique.

Étape 9 Cochez la case **Match Metrices** (Correspondance des mesures) pour redistribuer les routes avec la mesure spécifiée. Si vous spécifiez plusieurs mesures, les routes peuvent être mises en correspondance avec l'une ou l'autre des mesures.

Étape 10 Cochez la case **Match Tag Numbers** (Correspondance des numéros de balise) pour redistribuer les routes dans la table de routage qui correspondent aux balises spécifiées. Si vous spécifiez plusieurs numéros de balise, les routes peuvent être mises en correspondance avec l'une ou l'autre des mesures.

Étape 11 Cliquez sur OK.

Étape 12 Cliquez sur Apply (appliquer).

Configurer les filtres de chemin AS

Un filtre de chemin AS vous permet de filtrer le message de mise à jour de routage à l'aide de listes d'accès et d'examiner les préfixes individuels dans un message de mise à jour. Si un préfixe dans le message de mise à jour correspond aux critères de filtre, ce préfixe individuel est filtré ou accepté selon l'action configurée pour l'entrée de filtre. Cette section décrit les étapes requises pour configurer les filtres de chemin AS.

Remarque Les listes d'accès du chemin AS ne sont pas les mêmes que les ACL normales du pare-feu.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **AS Path Filters (Filtres de chemin AS)**.

Étape 2 Cliquez sur Add (ajouter).

La boîte de dialogue Add Filter (Ajouter un filtre) apparaît. À partir de cette boîte de dialogue, vous pouvez ajouter un nom de filtre, son accès à la redistribution (c'est-à-dire autoriser ou refuser) et son expression régulière.

Étape 3 Dans le champ Name (Nom), attribuez un nom au chemin de filtre AS.

Étape 4 Cliquez sur le bouton radio **Permit** (Autoriser) ou **Deny** (Refuser) pour indiquer l'accès à la redistribution.

Étape 5 Spécifiez l'expression régulière. Cliquez sur **Build** (Générer) pour créer une expression régulière.

Étape 6 Cliquez sur **Test** (Tester) pour tester si une expression régulière correspond à une chaîne de votre choix.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer les règles de communauté

Une communauté étendue est un groupe plus vaste de destinations partageant un attribut commun. Vous pouvez utiliser les listes de communautés pour créer des groupes de communautés à utiliser dans une clause de correspondance d'une feuille de route. Tout comme une liste d'accès, une série de listes de communautés peut être créée. Les instructions sont vérifiées jusqu'à ce qu'une correspondance soit trouvée. Dès qu'une instruction est satisfaite, le test est terminé. Cette section décrit les étapes requises pour configurer les règles de communauté.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **Community Rules (Règles de communauté)** > **.**

Étape 2 Cliquez sur Add (ajouter).

La boîte de dialogue Add Community Rule (Ajouter une règle de communauté) apparaît. À partir de cette boîte de dialogue, vous pouvez ajouter un nom de règle, un type de règle, son accès de redistribution (c'est-à-dire autoriser ou refuser) et des communautés spécifiques.

Étape 3 Dans le champ Rule Name (Nom de la règle), saisissez un nom pour la règle de communauté.

Étape 4 Cliquez sur le bouton radio Standard ou Expanded (Étendu) pour indiquer le type de règle de communauté.

Étape 5 Cliquez sur le bouton radio **Permit** (Autoriser) ou **Deny** (Refuser) pour indiquer l'accès à la redistribution.

Étape 6 Pour ajouter des règles de communauté standard :

a) Dans le champ Communautés, spécifiez un numéro de communauté. Les valeurs valides sont comprises entre 1 et 4294967200.

b) (Facultatif) Cochez la case Internet (communauté connue) pour spécifier la communauté Internet. Les routages de cette communauté sont annoncés à tous les homologues (internes et externes).

c) (Facultatif) Cochez la case Do not advertise to any peers (Ne pas annoncer aux homologues) (communauté connue) pour spécifier la communauté sans annonce. Les routages de cette communauté ne sont annoncés à aucun homologue (interne ou externe).
d) (Facultatif) Cochez la case Do not export to next AS (Ne pas exporter vers le prochain AS) (communauté connue) pour spécifier la communauté sans exportation. Les routes avec cette communauté sont annoncées uniquement aux homologues dans le même système autonome ou uniquement aux autres systèmes sous-autonomes d'une confédération. Ces routes ne sont pas annoncées aux homologues externes.

Étape 7 Pour ajouter des règles de communauté étendues :

a) Dans le champ**Regular Expression** (Expression régulière), saisissez une expression régulière. Sinon, cliquez sur **Build** (Générer) pour créer une expression régulière.
b) Cliquez sur **Test** (Tester) pour examiner si l'expression régulière créée correspond à une chaîne de votre choix.

Étape 8 Cliquez sur OK.

Étape 9 Cliquez sur Apply (appliquer).

Configurer les paramètres de la famille d'adresses IPv4

Les paramètres IPv4 pour le BGP peuvent être configurés à partir de l'option de famille IPv4 dans la configuration du BGP. La section de la famille IPv4 comprend des sous-sections pour les paramètres généraux, les paramètres d'adresse d'agrégation, les paramètres de filtrage et les paramètres de voisin. Chacune de ces sous-sections vous permet de personnaliser les paramètres propres à la famille IPv4.

Configurer les paramètres généraux de la famille IPv4

Cette section décrit les étapes requises pour configurer les paramètres IPv4 généraux.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur General (Général).

Le volet de configuration générale des paramètres BGP de la famille IPv4 s'affiche.

Étape 3 Spécifiez les distances externe, interne et locale dans la zone Administration Distances (Distances administratives).

Étape 4 Dans la liste déroulante Learning Routes Map (Carte de routage apprise), choisissez un nom de carte de routage. Cliquez sur **Manage** (Gérer) pour ajouter et configurer des cartes de routage.

Étape 5 (Facultatif) Cochez la case **Generate Default Route** (Générer une route par défaut) pour configurer un processus de routage BGP afin de distribuer une route par défaut (réseau 0.0.0.0).

Étape 6 (Facultatif) Cochez la case **Summarize subnet routes into network-level routes** (Résumé des routes de sous-réseau en routes de niveau réseau) pour configurer la synthèse automatique des routes de sous-réseau en routes de niveau réseau.

Étape 7 (Facultatif) Cochez la case **Advertise inactive routes** (Annoncer les routes inactives) pour annoncer les routes qui ne sont pas installées dans la base d'informations de routage (RIB).

Étape 8 (Facultatif) Cochez la case **Redistribute iBGP into an IGP** (Redistribuer l'IBGP dans un IGP) pour configurer la redistribution iBGP dans un protocole de passerelle intérieure (IGP), comme IS-IS ou OSPF.

Étape 9 (Facultatif) Saisissez un intervalle d'analyse (en secondes) pour les routeurs BGP pour la validation du saut suivant dans le champ **Scanning Interval** (Intervalle d'analyse). Les valeurs valides sont comprises entre 5 et 60 secondes.

Étape 10 (Facultatif) Cochez la case **Enable address tracking** (Activer le suivi des adresses) pour activer le suivi des adresses du saut suivant du BGP. Spécifiez l'intervalle de délai entre les vérifications sur les routes de saut suivant mises à jour et installées dans la table de routage dans le champ **Delay Interval** (Intervalle de délai).

Étape 11 (Facultatif) Spécifiez le nombre maximal de routes iBGP (Protocole Border Gateway Protocol) parallèles internes qui peuvent être installées dans une table de routage dans le champ **Number of Paths** (Nombre de chemins), puis cochez la case **iBGP multipaths** (Chemins multiples iBGP).

Étape 12 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres d'adresse globale de la famille IPv4

Cette section décrit les étapes requises pour définir l'agrégation de routes spécifiques en une seule route.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur **Aggregate Address** (Adresse agrégée).

Le volet de configuration des paramètres d'adresse agrégée s'affiche.

Étape 3 Cliquez sur **Add** (Ajouter).

Le volet Add Aggregate Address (Ajouter une adresse agrégée) s'affiche.

Étape 4 Spécifiez un objet réseau dans le champ **Network** (Réseau).

Étape 5 Cochez la case **Generate autonomous system set path information** (Générer des renseignements sur le chemin d'accès au système autonome) pour générer des renseignements sur le chemin d'accès au système autonome.

Étape 6 Cochez la case **Filters all more-specific routes from the updates** (Filtrer toutes les routes plus spécifiques à partir des mises à jour) pour filtrer toutes les routes plus spécifiques à partir des mises à jour.

Étape 7 Choisissez une carte de routage dans la liste déroulante Attribute Map (Carte d'attribut). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une carte de routage.

Étape 8 Choisissez une carte de routage dans la liste déroulante Advertise Map (Carte d'annonce). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une route.

Étape 9 Choisissez une carte de routage dans la liste déroulante Suppress Map (Carte de suppression). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une route.

Étape 10 Cliquez sur **OK**.

Étape 11 Spécifiez une valeur pour la minuterie d'agrégation (en secondes) dans le champ **Aggregate Timer** (Minuterie d'agrégation). Les valeurs valides sont 0 ou toute valeur comprise entre 6 et 60.

Étape 12 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de filtrage de la famille IPv4

Cette section décrit les étapes requises pour filtrer les routes ou les réseaux reçus dans les mises à jour BGP entrantes.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur **Filtering** (Filtrage).

Le volet Define filters for BGP updates (Définir les filtres pour les mises à jour du BGP) s'affiche.

Étape 3 Cliquez sur **Add** (ajouter).

Le volet Add Filter (Ajouter un filtre) s'affiche.

Étape 4 Choisissez une direction dans la liste déroulante Direction. La direction spécifie si le filtre doit être appliqué aux mises à jour entrantes ou sortantes.

Étape 5 Choisissez une liste d'accès standard dans la lise déroulante Access List (Liste d'accès). Cliquez sur **Manage** (Gérer) pour ajouter une nouvelle ACL.

Étape 6 Pour les filtres sortants, vous pouvez éventuellement spécifier les types de routes distribués.

a) Choisissez une option dans la liste déroulante Protocol (Protocole).

Vous pouvez choisir un protocole de routage, par exemple, **BGP**, **EIGRP**, **OSPF** ou **RIP**.

Choisissez **Connected** (Connecté) pour filtrer les homologues et les réseaux appris par le biais des routes connectées.

Choisissez **Static** (Statique) pour filtrer les homologues et les réseaux appris par le biais des routes statiques.

b) Si vous avez choisi BGP, EIGRP ou OSPF, choisissez également le **Process ID** (ID de processus) pour ce protocole.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de voisin BGP de la famille IPv4

Cette section décrit les étapes requises pour définir les voisins BGP et les paramètres de voisins.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** >**Routing (Routage)** **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur **Neighbor** (Voisin).

Étape 3 Cliquez sur **Add** (ajouter).

Étape 4 Cliquez sur **General** (Général) dans le volet de gauche.

Étape 5 Saisissez une adresse IP de voisin BGP dans le champ **IP Address** (Adresse IP). Cette adresse IP est ajoutée à la table des voisins BGP.

Étape 6 Saisissez le système autonome auquel le voisin BGP appartient dans le champ **Remote AS** (AS distant).

Étape 7 (Facultatif) Dans le champ **Description**, saisissez la description du voisin BGP.

Étape 8 (Facultatif) Cochez la case **Shutdown neighbor administratively** (Arrêter le voisin administrativement) pour désactiver un groupe de voisins ou d'homologues.

Étape 9 (Facultatif) Cochez la case **Enable address family** (Activer la famille d'adresses) pour activer la communication avec le voisin BGP.

Étape 10 (Facultatif) Cochez la case **Global Restart Functionality for this peer** (Fonctionnalité de redémarrage global pour cet homologue) pour activer ou désactiver la capacité de redémarrage progressif du protocole de passerelle frontière (BGP) pour un voisin ou un groupe d'homologues ASA.



Remarque Cette option est activée lorsque le périphérique est en mode haute disponibilité ou lorsqu'une grappe L2 (tous les nœuds du même réseau) est configurée.

Étape 11 (Facultatif) Pour mettre à jour une interface en tant que source pour le voisinage BGP, sélectionnez l'interface dans la liste déroulante **Update-Source** (Mettre à jour la source).



Remarque Si vous mettez à jour l'interface de boucle avec retour comme source pour le voisinage BGP, l'adresse IP de l'interface de boucle avec retour est annoncée sur le réseau. L'interface de boucle avec retour agit en tant qu'homologue eBGP et participe au routage. Comme l'interface de boucle avec retour est stable lorsqu'elle est activée et reste disponible jusqu'à ce qu'elle soit administrativement arrêtée, l'ASA est toujours accessible sur l'adresse IP de l'interface de boucle avec retour.

Étape 12 Cliquez sur **Filtering** (Filtrage) dans le volet de gauche.

Étape 13 (Facultatif) Choisissez la liste de contrôle d'accès entrant ou sortant appropriée dans la zone Filter routes using an access list (Filtrer les routes à l'aide d'une liste d'accès) pour distribuer les renseignements sur le voisin BGP. Cliquez sur **Manage** (Gérer) pour ajouter une ACL et des ACE au besoin.

Étape 14 (Facultatif) Choisissez les cartes de routage entrantes ou sortantes appropriées dans la zone Filter routes using a route map (Filtrer les routes à l'aide d'une carte de routage) pour appliquer une carte de routage aux routes entrantes ou sortantes. Cliquez sur **Manage** (Gérer) pour configurer une carte de routage.

Étape 15 (Facultatif) Choisissez la liste de préfixes entrants ou sortants appropriée dans la zone Filter routes using a prefix list (Filtrer les routes à l'aide d'une liste de préfixes) pour distribuer les renseignements sur le voisin BGP. Cliquez sur **Manage** (Gérer) pour configurer les listes de préfixes.

Étape 16 (Facultatif) Choisissez le filtre de chemin AS entrant ou sortant approprié dans la zone Filter routes using AS path filter (Filtrer les routes à l'aide d'un filtre de chemin AS) pour distribuer les renseignements sur le voisin BGP. Cliquez sur **Manage** (Gérer) pour configurer les filtres de chemin AS.

Étape 17 (Facultatif) Cochez la case **Limit the number of prefixes allowed from the neighbor** (Limiter le nombre de préfixes autorisés du voisin) pour contrôler le nombre de préfixes qui peuvent être reçus d'un voisin.

- Saisissez le nombre maximum de préfixes autorisés pour un voisin spécifique dans le champ **Maximum prefixes** (Nombre maximum de préfixes).

- Dans le champ **Threshold level** (Niveau de seuil), saisissez le pourcentage (du maximum) à partir duquel le routeur commence à générer un message d'avertissement. Les valeurs valides sont des entiers compris entre 1 et 100. La valeur par défaut est 75.
- (Facultatif) Cochez la case **Control prefixes received from a peer** (Contrôle des préfixes reçus d'un homologue) pour spécifier des contrôles supplémentaires pour les préfixes reçus d'un homologue. Effectuez l'une des opérations suivantes :
  - Cliquez sur **Terminate peering when prefix limit is exceeded** (Mettre fin au jumelage lorsque la limite de préfixes est dépassée) pour arrêter le voisin BGP lorsque la limite de préfixe est atteinte. Précisez l'intervalle après lequel le voisin BGP redémarrera dans le champ Restart interval (intervalle de redémarrage).
  - Cliquez sur **Give only warning message when prefix limit is exceeded** (Envoyer uniquement un message d'avertissement lorsque la limite de préfixe est dépassée) pour générer un message de journal lorsque la limite de préfixe maximale est dépassée. Dans ce cas, le voisin BGP ne sera pas interrompu.

Étape 18 Cliquez sur **Routes** dans le volet de gauche.

Étape 19 Saisissez l'intervalle minimal (en secondes) entre l'envoi des mises à jour de routage de BGP dans le champ **Advertisement Interval** (intervalle des annonces).

Étape 20 (Facultatif) Cochez la case **Generate Default route** (Générer une route par défaut) pour permettre au routeur local d'envoyer la route par défaut 0.0.0.0 à un voisin pour qu'il l'utilise comme route par défaut.

- Choisissez la carte de routage qui permet l'injection conditionnelle de la route 0.0.0.0 dans la liste déroulante Route map (Carte de routage). Cliquez sur **Manage** (Gérer) pour ajouter et configurer une carte de routage.

Étape 21 (Facultatif) Pour ajouter des routes annoncées sous condition, procédez comme suit :

a) Cliquez sur **Add** (Ajouter) dans la section Conditionly Advertise Routes (Routes annoncées sous condition).
b) Choisissez la carte de routage qui sera annoncée dans la liste déroulante Advertise Map (Carte d'annonce) si les conditions de la carte existante ou inexistante sont remplies.
c) Effectuez l'une des opérations suivantes :
   - Cliquez sur **Exist Map** (Carte existante) et choisissez une carte de routage. Cette carte de routage sera comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
   - Cliquez sur **Non-exist Map** (Carte non existante) et choisissez une carte de routage. Cette carte de routage sera comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
d) Cliquez sur **Ok**.

Étape 22 (Facultatif) Cochez la case **Remove private autonomous system (AS) numbers from outbound routing updates** (Supprimer les numéros de systèmes autonomes (AS) privés des mises à jour de routage sortantes) pour empêcher les numéros de système autonomes privés d'être annoncés sur les routes sortantes.

Étape 23 Cliquez sur **Timers** (Minuteries) dans le volet de gauche.

Étape 24 (Facultatif) Cochez la case Set timers for the BGP peer (Définir les minuteries pour l'homologue BGP) pour définir la fréquence keepalive, le délai de rétention et le délai de rétention minimum.

- Saisissez la fréquence (en secondes) à laquelle l'ASA envoie des messages keepalive au voisin dans le champ **Keepalive frequency** (Fréquence keepalive). Les valeurs valides sont comprises entre 0 et 65 535. La valeur par défaut est 60 secondes.
- Dans le champ **Hold time** (Délai de rétention), saisissez l'intervalle (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort. La valeur par défaut est 180secondes.
- (Facultatif) Dans le champ Min Hold time (Délai de rétention min.), saisissez l'intervalle minimum (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort.



Remarque Une durée d'attente de moins de 20 secondes augmente les risques d'intermittence des pairs

Étape 25 Cliquez sur Advanced (Avancé) dans le volet de gauche.

Étape 26 (Facultatif) Cochez la case Enable Authentication (activer l'authentification) pour activer l'authentification MD5 sur une connexion TCP entre deux homologues BGP.

- Choisissez un type de chiffrement dans la liste déroulante Encryption Type (Type de chiffrement).
- Saisissez un mot de passe dans le champ **Password** (Mot de passe). Saisissez à nouveau le mot de passe dans le champ **Confirm Password** (Confirmer le mot de passe).

  Le mot de passe est sensible à la casse et peut comporter jusqu'à 25 caractères lorsque la commande service password-encryption est activée et jusqu'à 81 caractères lorsqu'elle ne l'est pas. La chaîne peut contenir n'importe quel caractère alphanumérique, y compris des espaces. Vous ne pouvez pas spécifier de mot de passe au format nombre-espace-caractère quelconque. L'espace après le numéro peut faire échouer l'authentification.

Étape 27 (Facultatif) Cochez la case **Send Community Attribute to this neighbor** (Envoyer l'attribut de communauté à ce voisin).

Étape 28 (Facultatif) Cochez la case **Use ASA as next hop for neighbor** (Utiliser l'ASA comme prochain saut pour le voisin) pour configurer le routeur comme prochain saut pour un voisin ou un groupe d'homologues qui communique avec BGP.

Étape 29 Effectuez l'une des opérations suivantes :

- Cliquez sur **Allow connections with neighbor that is not directly connected** (Autoriser les connexions avec le voisin qui n'est pas directement connecté) pour accepter et tenter des connexions BGP avec des homologues externes résidant sur des réseaux qui ne sont pas connectés directement.
  - (Facultatif) Saisissez la durée de vie dans le champ **TTL hops** (Sauts TTL). Les valeurs valides sont comprises entre 1 et 255.
  - (Facultatif) Cochez la case **Disable connection verification** (Désactiver la vérification de connexion) pour désactiver la vérification de connexion afin d'établir une session d'homologation eBGP avec un homologue à saut unique qui utilise une interface de boucle avec retour.
- Cliquez sur **Limit number of TTL hops to neighbor** (Limiter le nombre de sauts TTL vers le voisin) pour vous permettre de sécuriser une session d'homologation BGP.

- Saisissez le nombre maximal de sauts qui séparent les homologues eBGP dans le champ **Sauts TTL**. Les valeurs valides sont comprises entre 1 et 254.

Étape 30 (Facultatif) Dans le champ **Weight** (Pondération), saisissez une pondération pour la connexion du voisin BGP.

Étape 31 Choisissez la version BGP que l'ASA acceptera dans la liste déroulante **BGP version** (Version BGP).



Remarque La version peut être définie sur 2 pour forcer le logiciel à utiliser uniquement la version 2 avec le voisin spécifié. La valeur par défaut est d'utiliser la version 4 et de négocier dynamiquement à la baisse jusqu'à la version 2 si nécessaire.

Étape 32 (Facultatif) Cochez la case **TCP Path MTU Discovery** (Découverte MTU du chemin TCP) pour activer une session de transport TCP pour une session BGP.

Étape 33 Choisissez le **TCP connection mode** (Mode de connexion TCP) dans la liste déroulante du mode de transport TCP.

Étape 34 Cliquez sur **Migration** dans le volet gauche.

Étape 35 (Facultatif) Cochez la case **Customize the AS number for routes received from the neighbor** (Personnaliser le numéro AS pour les routes reçues du voisin) pour personnaliser l'attribut AS_PATH pour les routes reçues d'un voisin eBGP.

- Saisissez le numéro du système autonome local dans le champ **Local AS Number** (Numéro AS local). Les valeurs valides sont comprises entre 1 et 65 535.
- (Facultatif) Cochez la case **Do not prepend local AS number for routes received from neighbor** (Ne pas ajouter au début le numéro AS local pour les routes reçues du voisin). Le numéro AS local ne sera pas ajouté au début des routes reçues de l'homologue eBGP.
- (Facultatif) Cochez la case **Replace real AS number with local AS number in routes received from neighbor** (Remplacer le numéro AS réel par le numéro AS local dans les routes reçues du voisin). Le numéro AS du processus de routage local n'est pas ajouté au début.
- (Facultatif) Cochez la case **Accept either real AS number or local AS number in routes received from neighbor** (Accepter le numéro AS réel ou le numéro AS local dans les routes reçues du voisin).

Étape 36 Cliquez sur **OK**.

Étape 37 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres réseau IPv4

Cette section décrit les étapes requises pour définir les réseaux à annoncer par le processus de routage de BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur **Networks** (Réseaux).

Le volet Define networks to be advertised by the BGP routing process configuration (Définir les réseaux à annoncer par la configuration du processus de routage BGP) s'affiche.

Étape 3 Cliquez sur **Add** (ajouter).

Le volet Add Network (ajouter un réseau) s'affiche.

Étape 4 Spécifiez le réseau que BGP annoncera dans le champ **Address** (Adresse).



Remarque Pour qu'un préfixe de réseau soit annoncé, une voie de routage vers le périphérique doit exister dans la table de routage.

Étape 5 (Facultatif) Choisissez un masque de réseau ou de sous-réseau dans la liste déroulante **Netmask** (Masque réseau).

Étape 6 Choisissez une carte de routage qui doit être examinée pour filtrer les réseaux à annoncer dans la liste déroulante **Route Map**. Cliquez sur Manage (Gérer) pour configurer ou ajouter une carte de routage.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de redistribution IPv4

Cette section décrit les étapes nécessaires pour définir les conditions de redistribution des routes d'un autre domaine de routage vers BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)** > **.**

Étape 2 Cliquez sur **Redistribution**.

Le volet Redistribution s'affiche.

Étape 3 Cliquez sur **Add** (Ajouter).

Le volet Add Redistribution (ajouter une redistribution) s'affiche.

Étape 4 Choisissez le protocole à partir duquel vous souhaitez redistribuer les routes dans le domaine BGP dans la liste déroulante **Source Protocol** (Protocole source).

Étape 5 Choisissez un ID de processus pour le protocole source dans la liste déroulante **Process ID** (ID de processus).

Étape 6 (Facultatif) Saisissez une mesure pour la route redistribuée dans le champ **Metric** (Mesure).

Étape 7 Choisissez une carte de routage qui doit être examinée pour filtrer les réseaux à annoncer dans la liste déroulante **Route Map** (Carte de routage). Cliquez sur **Manage** (Gérer) pour configurer ou ajouter une carte de routage.

Étape 8 Cochez une ou plusieurs des cases **Internal** (Interne), **External** (Externe) et **NSSA External match** (Correspondance externe de NSSA) pour redistribuer les routes à partir d'un réseau OSPF.

Cette étape s'applique uniquement à la redistribution à partir des réseaux OSPF.

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres d'injection de route IPv4

Cette section décrit les étapes nécessaires pour définir les routes à injecter de manière conditionnelle dans la table de routage de BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)** > **.**

Étape 2 Cliquez sur **Route Injection** (Injection de route).

Le volet Route Injection (Injection de routage) s'affiche.

Étape 3 Cliquez sur **Add** (Ajouter).

Le volet Add Conditionally injected route (Ajouter une route injectée sous condition) s'affiche.

Étape 4 Choisissez la carte de routage qui spécifie les préfixes à injecter dans la table de routage de BGP locale depuis la liste déroulante **Inject Map** (Carte d'injection).

Étape 5 Choisissez la carte de routage contenant les préfixes que le locuteur BGP suivra depuis la liste déroulante **Exist Map** (Carte existante).

Étape 6 Cochez la case **Injected routes will inherit the attributes of the aggregate route** (Les routes injectées hériteront des attributs de la route agrégée) pour configurer la route injectée pour qu'elle hérite des attributs de la route agrégée.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de la famille d'adresses IPv6

Les paramètres IPv6 pour le BGP peuvent être configurés à partir de l'option de famille IPv6 dans la configuration du BGP. La section de la famille IPv6 comprend des sous-sections pour les paramètres généraux, les paramètres d'adresse d'agrégation et les paramètres de voisin. Chacune de ces sous-sections vous permet de personnaliser les paramètres propres à la famille IPv6.

Cette section décrit comment personnaliser les paramètres de famille IPv6 du BGP.

Configurer les paramètres généraux de la famille IPv6

Cette section décrit les étapes requises pour configurer les paramètres IPv6 généraux.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family**. (Configuration > Configuration du périphérique > Routage > GBP > Famille IPv6).

Étape 2 Cliquez sur **General** (Général).

Le volet de configuration générale des paramètres BGP de la famille IPv6 s'affiche.

Étape 3 Spécifiez les distances externe, interne et locale dans la zone **Administration Route Distances** (Distances de la route administrative).

Étape 4 (Facultatif) Cochez la case **Generate Default Route** (Générer une route par défaut) pour configurer un processus de routage BGP afin de distribuer une route par défaut (réseau 0.0.0.0).

Étape 5 (Facultatif) Cochez la case **Advertise inactive routes** (Annoncer les routes inactives) pour annoncer les routes qui ne sont pas installées dans la base d'informations de routage (RIB).

Étape 6 (Facultatif) Cochez la case **Redistribute iBGP into an IGP** (Redistribuer l'IBGP dans un IGP) pour configurer la redistribution iBGP dans un protocole de passerelle intérieure (IGP), comme IS-IS ou OSPF.

Étape 7 (Facultatif) Saisissez un intervalle d'analyse (en secondes) pour les routeurs BGP pour la validation du saut suivant dans le champ **Scanning Interval** (Intervalle d'analyse). Les valeurs valides sont comprises entre 5 et 60 secondes.

Étape 8 (Facultatif) Spécifiez le nombre maximum de routes de protocole de passerelle frontière qui peuvent être installées dans une table de routage dans le champ **Number of paths** (Nombre de chemins).

Étape 9 (Facultatif) Cochez la case **IBGP multipaths** (Chemins multiples IBGP) et spécifiez le nombre maximum de routes iBGP (Protocole Border Gateway Protocol) parallèles internes qui peuvent être installées dans une table de routage dans le champ **Number of paths** (Nombre de chemins).

Étape 10 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres d'adresse globale de la famille IPv6

Cette section décrit les étapes requises pour définir l'agrégation de routes spécifiques en une seule route.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family**. (Configuration > Configuration du périphérique > Routage > GBP > Famille IPv6).

Étape 2 Cliquez sur **Aggregate Address** (Adresse agrégée).

Le volet de configuration des paramètres d'adresse agrégée s'affiche.

Étape 3 Cliquez sur **Add** (Ajouter).

Le volet Add Aggregate Address (Ajouter une adresse agrégée) s'affiche.

Étape 4 Indiquez une adresse IPv6 dans le champ **IPv6/Address Mask** (IPv6/Masque d'adresse). Par ailleurs, parcourez la liste pour ajouter un objet réseau.

Étape 5 Cochez la case **Generate autonomous system set path information** (Générer des renseignements sur le chemin d'accès au système autonome) pour générer des renseignements sur le chemin d'accès au système autonome. Le chemin annoncé pour cette route sera un AS_SET composé de tous les éléments contenus dans tous les chemins résumés.



Remarque N'utilisez pas cette forme de commande aggregate-address lors de l'agrégation de nombreux chemins, car cette route doit être continuellement retirée et mise à jour en tant que renseignements sur l'accessibilité du chemin au système autonome pour les modifications de routes résumées.

Étape 6 Cochez la case **Filters all more-specific routes from the updates** (Filtrer toutes les routes plus spécifiques à partir des mises à jour) pour filtrer toutes les routes plus spécifiques à partir des mises à jour. Cela crée non seulement la route agrégée, mais supprime également les annonces de routes plus spécifiques à tous les voisins.

Étape 7 Choisissez une carte de routage dans la liste déroulante **Attribute Map** (Carte d'attribut). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une carte de routage. Cela permet de modifier les attributs de la route agrégée.

Étape 8 Choisissez une carte de routage dans la liste déroulante **Advertise Map** (Carte d'annonce). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une route. Cela sélectionne des routes spécifiques qui seront utilisées pour créer différents composants de la route agrégée.

Étape 9 Choisissez une carte de routage dans la liste déroulante **Suppress Map** (Carte de suppression). Cliquez sur **Manage** (Gérer) pour ajouter ou configurer une route. Cela crée la route agrégée, mais supprime l'annonce des routes spécifiées.

Étape 10 Cliquez sur **OK**.

Étape 11 Spécifiez une valeur pour la minuterie d'agrégation (en secondes) dans le champ **Aggregate Timer** (Minuterie d'agrégation). Les valeurs valides sont 0 ou toute valeur comprise entre 6 et 60. Cela spécifie l'intervalle auquel les routes seront agrégées. La valeur par défaut est de 30 secondes.

Étape 12 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de voisin BGP de la famille IPv6

Cette section décrit les étapes requises pour définir les voisins BGP et les paramètres de voisins.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv6 Family (Famille IPv6)**

Étape 2 Cliquez sur **Neighbor** (Voisin).

Étape 3 Cliquez sur **Add** (Ajouter).

Étape 4 Cliquez sur **General** (Général) dans le volet de gauche.

Étape 5 Saisissez une adresse IPv6 de voisin BGP dans le champ **IPv6 Address** (Adresse IPv6). Cette adresse IPv6 est ajoutée à la table des voisins BGP.

Étape 6 Saisissez le système autonome auquel le voisin BGP appartient dans le champ **Remote AS** (AS distant).

Étape 7 (Facultatif) Dans le champ **Description**, saisissez la description du voisin BGP.

Étape 8 (Facultatif) Cochez la case **Shutdown neighbor administratively** (Arrêter le voisin administrativement) pour désactiver un groupe de voisins ou d'homologues.

Étape 9 (Facultatif) Cochez la case **Enable address family** (Activer la famille d'adresses) pour activer la communication avec le voisin BGP.

Étape 10 (Facultatif) Cochez la case **Global Restart Functionality for this peer** (Fonctionnalité de redémarrage global pour cet homologue) pour activer ou désactiver la capacité de redémarrage progressif du protocole de passerelle frontière (BGP) pour un voisin ou un groupe d'homologues ASA.



Remarque Cette option est activée lorsque le périphérique est en mode haute disponibilité ou lorsqu'une grappe L2 (tous les nœuds du même réseau) est configurée.

Étape 11 (Facultatif) Pour mettre à jour une interface en tant que source pour le voisinage BGP, sélectionnez l'interface dans la liste déroulante **Update-Source** (Mettre à jour la source).



Remarque Si vous mettez à jour l'interface de boucle avec retour comme source pour le voisinage BGP, l'adresse IP de l'interface de boucle avec retour est annoncée sur le réseau. L'interface de boucle avec retour agit en tant qu'homologue eBGP et participe au routage. Comme l'interface de boucle avec retour est stable lorsqu'elle est activée et reste disponible jusqu'à ce qu'elle soit administrativement arrêtée, l'ASA est toujours accessible sur l'adresse IP de l'interface de boucle avec retour.

Étape 12 Cliquez sur **Filtering** (Filtrage) dans le volet de gauche.

Étape 13 (Facultatif) Choisissez les cartes de routage entrantes ou sortantes appropriées dans la zone **Filter routes using a route map** (Filtrer les routes à l'aide d'une carte de routage) pour appliquer une carte de routage aux routes entrantes ou sortantes. Cliquez sur **Manage** (Gérer) pour configurer une carte de routage.

Étape 14 (Facultatif) Choisissez la liste de préfixes entrants ou sortants appropriée dans la zone **Filter routes using a prefix list** (Filtrer les routes à l'aide d'une liste de préfixes) pour distribuer les renseignements sur le voisin BGP. Cliquez sur **Manage** (Gérer) pour configurer les listes de préfixes.

Étape 15 (Facultatif) Choisissez le filtre de chemin AS entrant ou sortant approprié dans la zone **Filter routes using AS path filter** (Filtrer les routes à l'aide d'un filtre de chemin AS) pour distribuer les renseignements sur le voisin BGP. Cliquez sur **Manage** (Gérer) pour configurer les filtres de chemin AS.

Étape 16 (Facultatif) Cochez la case **Limit the number of prefixes allowed from the neighbor** (Limiter le nombre de préfixes autorisés du voisin) pour contrôler le nombre de préfixes qui peuvent être reçus d'un voisin.

Étape 17 Saisissez le nombre maximum de préfixes autorisés pour un voisin spécifique dans le champ **Maximum prefixes** (Nombre maximum de préfixes).

Étape 18 Dans le champ **Threshold level** (Niveau de seuil), saisissez le pourcentage (du maximum) à partir duquel le routeur commence à générer un message d'avertissement. Les valeurs valides sont des entiers compris entre 1 et 100. La valeur par défaut est 75.

Étape 19 (Facultatif) Cochez la case **Control prefixes received from a peer** (Contrôle des préfixes reçus d'un homologue) pour spécifier des contrôles supplémentaires pour les préfixes reçus d'un homologue. Effectuez l'une des opérations suivantes :

- Cliquez sur **Terminate peering when prefix limit is exceeded** (Mettre fin au jumelage lorsque la limite de préfixes est dépassée) pour arrêter le voisin BGP lorsque la limite de préfixe est atteinte. Précisez l'intervalle après lequel le voisin BGP redémarrera dans le champ **Restart interval** (intervalle de redémarrage).

- Cliquez sur **Give only warning message when prefix limit is exceeded** (Envoyer uniquement un message d'avertissement lorsque la limite de préfixe est dépassée) pour générer un message de journal lorsque la limite de préfixe maximale est dépassée. Dans ce cas, le voisin BGP ne sera pas interrompu.

Étape 20 Cliquez sur **Routes** dans le volet de gauche.

Étape 21 Saisissez l'intervalle minimum (en secondes) entre l'envoi des mises à jour de routage BGP dans le champ **Advertisement Interval** (Intervalle des annonces).

Étape 22 (Facultatif) Cochez la case **Generate Default route** (Générer une route par défaut) pour permettre au routeur local d'envoyer la route par défaut 0.0.0.0 à un voisin pour qu'il l'utilise comme route par défaut.

Étape 23 Choisissez la carte de routage qui permet l'injection conditionnelle de la route 0.0.0.0 dans la liste déroulante **Route map** (Carte de routage). Cliquez sur **Manage** (Gérer) pour ajouter et configurer une carte de routage.

Étape 24 (Facultatif) Pour ajouter des routes annoncées sous condition, procédez comme suit :

a) Cliquez sur **Add** (Ajouter) dans la section Conditionly Advertise Routes (Routes annoncées sous condition).

b) Choisissez la carte de routage qui sera annoncée dans la liste déroulante **Advertise Map** (Carte d'annonce) si les conditions de la carte existante ou inexistante sont remplies.

c) Effectuez l'une des opérations suivantes :

- Cliquez sur **Exist Map** (Carte existante) et choisissez une carte de routage. Cette carte de routage sera comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
- Cliquez sur **Non-exist Map** (Carte non existante) et choisissez une carte de routage. Cette carte de routage sera comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.

d) Cliquez sur **Ok**.

Étape 25 (Facultatif) Cochez la case **Remove private autonomous system (AS) numbers from outbound routing updates** (Supprimer les numéros de systèmes autonomes (AS) privés des mises à jour de routage sortantes) pour empêcher les numéros de système autonomes privés d'être annoncés sur les routes sortantes.

Étape 26 Cliquez sur **Timers** (Minuteries) dans le volet de gauche.

Étape 27 (Facultatif) Cochez la case **Set timers for the BGP peer** (Définir les minuteries pour l'homologue BGP) pour définir la fréquence keepalive, le délai de rétention et le délai de rétention minimum.

Étape 28 Saisissez la fréquence (en secondes) à laquelle l'ASA envoie des messages keepalive au voisin dans le champ **Keepalive frequency** (Fréquence keepalive). Les valeurs valides sont comprises entre 0 et 65 535. La valeur par défaut est 60 secondes.

Étape 29 Dans le champ **Hold time** (Délai de rétention), saisissez l'intervalle (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort. La valeur par défaut est 180secondes.

Étape 30 (Facultatif) Dans le champ **Min Hold time** (Délai de rétention min.), saisissez l'intervalle minimum (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort.

Remarque Une durée d'attente de moins de 20 secondes augmente les risques d'intermittence des pairs

Étape 31 Cliquez sur **Advanced** (Avancé) dans le volet de gauche.

Étape 32 (Facultatif) Cochez la case **Enable Authentication** (Activer l'authentification) pour activer l'authentification MD5 sur une connexion TCP entre deux homologues BGP.

Étape 33 Choisissez un type de chiffrement dans la liste déroulante **Encryption Type** (Type de chiffrement).

Étape 34 Saisissez un mot de passe dans le champ **Password** (Mot de passe). Saisissez votre nouveau mot de passe dans le champ **Confirm Password** (Confirmer le mot de passe).

Le mot de passe est sensible à la casse et peut comporter jusqu'à 25 caractères lorsque la commande service password-encryption est activée et jusqu'à 81 caractères lorsqu'elle ne l'est pas. La chaîne peut contenir n'importe quel caractère alphanumérique, y compris des espaces. Vous ne pouvez pas spécifier de mot de passe au format nombre-espace-caractère quelconque. L'espace après le numéro peut faire échouer l'authentification.

Étape 35 (Facultatif) Cochez la case **Send Community Attribute to this neighbor** (Envoyer l'attribut de communauté à ce voisin).

Étape 36 (Facultatif) Cochez la case **Use ASA as next hop for neighbor** (Utiliser l'ASA comme prochain saut pour le voisin) pour configurer le routeur comme prochain saut pour un voisin ou un groupe d'homologues qui communique avec BGP.

Étape 37 Effectuez l'une des opérations suivantes :

- Cliquez sur **Allow connections with neighbor that is not directly connected** (Autoriser les connexions avec le voisin qui n'est pas directement connecté) pour accepter et tenter des connexions BGP avec des homologues externes résidant sur des réseaux qui ne sont pas connectés directement.
  - (Facultatif) Saisissez la durée de vie dans le champ **TTL hops** (Sauts TTL). Les valeurs valides sont comprises entre 1 et 255.
  - (Facultatif) Cochez la case **Disable connection verification** (Désactiver la vérification de connexion) pour désactiver la vérification de connexion afin d'établir une session d'homologation eBGP avec un homologue à saut unique qui utilise une interface de boucle avec retour.
- Cliquez sur **Limit number of TTL hops to neighbor** (Limiter le nombre de sauts TTL vers le voisin) pour vous permettre de sécuriser une session d'homologation BGP. Saisissez le nombre maximal de sauts qui séparent les homologues eBGP dans le champ Sauts TTL. Les valeurs valides sont comprises entre 1 et 254.

Étape 38 (Facultatif) Dans le champ **Weight** (Pondération), saisissez une pondération pour la connexion du voisin BGP.

Étape 39 Choisissez la version BGP que l'ASA acceptera dans la liste déroulante BGP version (Version BGP).



Remarque La version peut être définie sur 2 pour forcer le logiciel à utiliser uniquement la version 2 avec le voisin spécifié. La valeur par défaut est d'utiliser la version 4 et de négocier dynamiquement à la baisse jusqu'à la version 2 si nécessaire.

Étape 40 (Facultatif) Cochez la case **TCP Path MTU Discovery** (Découverte MTU du chemin TCP) pour activer une session de transport TCP pour une session BGP.

Étape 41 Choisissez le **TCP connection mode** (Mode de connexion TCP) dans la liste déroulante du mode de transport TCP.

Étape 42 Cliquez sur **Migration** dans le volet gauche.

Étape 43 (Facultatif) Cochez la case **Customize the AS number for routes received from the neighbor** (Personnaliser le numéro AS pour les routes reçues du voisin) pour personnaliser l'attribut AS_PATH pour les routes reçues d'un voisin eBGP.

- Saisissez le numéro du système autonome local dans le champ Local AS Number (Numéro AS local). Les valeurs valides sont comprises entre 1 et 65 535.
- (Facultatif) Cochez la case Do not prepend local AS number for routes received from neighbor (Ne pas ajouter au début le numéro AS local pour les routes reçues du voisin). Le numéro AS local ne sera pas ajouté au début des routes reçues de l'homologue eBGP.
- (Facultatif) Cochez la case Replace real AS number with local AS number in routes received from neighbor (Remplacer le numéro AS réel par le numéro AS local dans les routes reçues du voisin). Le numéro AS du processus de routage local n'est pas ajouté au début.
- (Facultatif) Cochez la case Accept either real AS number or local AS number in routes received from neighbor (Accepter le numéro AS réel ou le numéro AS local dans les routes reçues du voisin).

Étape 44 Cliquez sur **OK**.

Étape 45 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres réseau IPv6

Cette section décrit les étapes requises pour définir les réseaux à annoncer par le processus de routage de BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family**. (Configuration > Configuration du périphérique > Routage > GBP > Famille IPv6).

Étape 2 Cliquez sur **Networks** (Réseaux).

Le volet Define the networks to be advertised by the BGP routing process configuration (Définir les réseaux à annoncer par la configuration du processus de routage BGP) s'affiche.

Étape 3 Cliquez sur **Add** (ajouter).

Le volet Add Network (ajouter un réseau) s'affiche.

Étape 4 (Facultatif) Dans le champ Prefix Name (nom du préfixe), précisez le nom de préfixe du client de délégation de préfixe DHCPv6 (voir Activer le client de délégation de préfixe IPv6, à la page 711).

Étape 5 Dans le champ**IPv6 Address/mask (adresse/masque IPv6**), précisez le réseau que BGP annoncera.

Si vous spécifiez le **nom de préfixe**, saisissez le préfixe et le masque de sous-réseau; le réseau annoncé se compose du préfixe délégué + du préfixe de sous-réseau.

Étape 6 Choisissez une carte de routage qui doit être examinée pour filtrer les réseaux à annoncer dans la liste déroulante **Route Map**. Cliquez éventuellement sur **Manage** (Gérer) pour configurer ou ajouter une carte de routage.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de redistribution IPv6

Cette section décrit les étapes nécessaires pour définir les conditions de redistribution des routes d'un autre domaine de routage vers BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family**. (Configuration > Configuration du périphérique > Routage > GBP > Famille IPv6).

Étape 2 Cliquez sur Redistribution.

Étape 3 Cliquez sur Add (ajouter).

Le volet Add Redistribution (ajouter une redistribution) s'affiche.

Étape 4 Dans la iste déroulante Source Protocol (Protocole source), choisissez le protocole à partir duquel vous souhaitez redistribuer les routes dans le domaine BGP.

Étape 5 Dans la liste déroulante Process ID (ID de processus), choisissez un ID de processus pour le protocole source. Cette option est disponible uniquement pour le protocole source OSPF.

Étape 6 (Facultatif) Dans le champ Metric (Mesure), saisissez une mesure pour la route redistribuée.

Étape 7 Dans la liste déroulante Route Map (Carte de routage), choisissez une carte de routage qui doit être examinée pour filtrer les réseaux à redistribuer. Cliquez sur Manage (Gérer) pour configurer ou ajouter une carte de routage.

Étape 8 Cochez une ou plusieurs des cases Match (Correspondance) (interne, externe 1, externe 2, NSSA externe 1 et NSSA externe 2) pour redistribuer les routes à partir d'un réseau OSPF.

Cette étape s'applique uniquement à la redistribution à partir des réseaux OSPF.

Étape 9 Cliquez sur OK.

Étape 10 Cliquez sur Apply (appliquer).

Configurer les paramètres d'injection de route IPv6

Cette section décrit les étapes nécessaires pour définir les routes à injecter de manière conditionnelle dans la table de routage de BGP.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family (Famille IPv4)**.

Étape 2 Cliquez sur **Route Injection** (Injection de route).

Étape 3 Cliquez sur **Add** (Ajouter).

Le volet Add Conditionally injected route (Ajouter une route injectée sous condition) s'affiche.

Étape 4 Dans la liste déroulante **Inject Map** (Carte d'injection), choisissez la carte de routage qui spécifie les préfixes à injecter dans la table de routage de BGP locale.

Étape 5 Dans la liste déroulante**Exist Map** (Carte existante), choisissez la carte de routage contenant les préfixes que le locuteur BGP suivra.

Étape 6 Cochez la case **Injected routes will inherit the attributes of the aggregate route** (Les routes injectées hériteront des attributs de la route agrégée) pour configurer la route injectée pour qu'elle hérite des attributs de la route agrégée.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Supervision BGP

Vous pouvez utiliser les commandes suivantes pour superviser le processus de routage BGP. Pour obtenir des exemples et des descriptions de la sortie de la commande, consultez la référence de commande. En outre, vous pouvez désactiver la journalisation des messages de modification de voisin et des messages d'avertissement de voisin.

Pour superviser diverses statistiques de routage BGP, saisissez l'une des commandes suivantes :



Remarque Pour désactiver les messages du journal BGP, saisissez la commande **no bgp log-neighbor-changes** dans le mode de configuration du routeur. Cela désactive la journalisation des messages de modification de voisin. Saisissez cette commande en mode de configuration du routeur pour le processus de routage BGP. Par défaut, les modifications de voisins sont journalisées.

- **Monitoring (Supervision) > Routing (Routage) > BGP Neighbors (Voisins BGP)**

  Chaque ligne représente un voisin BGP. Pour chaque voisin, la liste comprend l'adresse IP, le numéro d'AS, l'ID de routeur, l'état (actif, inactif, etc.), la disponibilité, la capacité de redémarrage progressif, l'heure de redémarrage et l'heure du chemin obsolète.

- **Monitoring (Supervision) > Routing (Routage) > BGP Routes (Routes BGP)**

  Chaque ligne représente une route BGP. Pour chaque route, la liste comprend le code d'état, l'adresse IP, l'adresse du saut suivant, la mesure de la route, les valeurs de préférence locales, la pondération et le chemin.

Historique de BGP

Tableau 41 : Historique des fonctionnalités de BGP

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge BGP	9.2(1)	Une prise en charge a été ajoutée pour le routage des données, l'exécution de l'authentification, ainsi que la redistribution et la supervision des informations de routage à l'aide du protocole de passerelle frontière. Nous avons introduit les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP Monitoring (Supervision BGP) > Routing (Routage) > BGP Neighbors (Voisins BGP), Monitoring (Supervision) > Routing (Routage) > BGP Routes (Routes BGP) Nous avons modifié les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Static Routes (Routes statiques) > Add (Ajouter) > Add Static Route (Ajouter une route statique) Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage) > Add (Ajouter) > Add Route Map (Ajouter une carte de routage)
Prise en charge BGP pour la mise en grappe d'ASA	9.3(1)	Nous avons ajouté la prise en charge de la mise en grappe de niveau 2 et de niveau 3. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > IPv4 Family (Famille IPv4) > General (Général)
Prise en charge BGP pour la transmission sans interruption	9.3(1)	Nous avons ajouté la prise en charge de la transmission sans interruption. Nous avons modifié les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > General (Général), Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > IPv4 Family (Famille IPv4) > Neighbor (Voisin), Monitoring (Supervision) > Routing (Routage) > BGP Neighbors (Voisins BGP)
Prise en charge BGP pour les cartes annoncées	9.3(1)	Nous avons ajouté la prise en charge des cartes annoncées BGPv4. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > IPv4 Family (Famille IPv4) > Neighbor (Voisin) > Add BGP Neighbor (Ajouter un voisin BGP) > Routes

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge BGP pour IPv6	9.3(2)	Nous avons ajouté la prise en charge d'IPv6. Nous avons introduit l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > BGP > IPv6 Family (Famille IPv6)
Annonce de réseau IPv6 pour les préfixes délégués	9.6(2)	L'ASA prend désormais en charge le client de délégation de préfixe DHCPv6. L'ASA obtient le ou les préfixes délégués d'un serveur DHCPv6. L'ASA peut ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface ASA afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. Vous pouvez configurer le routeur BGP pour annoncer ces préfixes. Nous avons modifié l'écran suivant : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv6 Family (Famille IPv6)** > **Networks (Réseaux)**
Prise en charge de l'interface de boucle avec retour pour le trafic BGP	9.18(2)	Vous pouvez utiliser une interface de boucle avec retour pour le trafic BGP. Commandes nouvelles/modifiées : **interface loopback**, **neighbor update-source** Écrans Nouveaux ou modifiés : • **Configuration (configuration)** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add Loopback Interface (Ajouter une interface de boucle avec retour)**. • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv4 Family/IPv6 Family (Famille IPv4/famille IPv6)** > **Neighbor (Voisin)** > **Add (Ajouter)** > **General (Général)** La prise en charge d'ASDM a été ajoutée dans la version 7.19.
Prise en charge du redémarrage progressif pour IPv6	9.19(1)	Nous avons ajouté la prise en charge du redémarrage progressif pour la famille d'adresses IPv6.



CHAPITRE 34

OSPF

Ce chapitre décrit comment configurer l'ASA pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole de routage Open Shortest Path First (OSPF).

- Routage OSPF, à la page 931
- Directives pour OSPF, à la page 935
- Configurer le protocole OSPFv2, à la page 938
- Configurer l'ID de routeur OSPFv2, à la page 941
- Personnaliser le protocole OSPFv2, à la page 943
- Configurer le protocole OSPFv3, à la page 963
- Configurer le redémarrage progressif, à la page 974
- Exemple de protocole OSPFv2, à la page 979
- Exemples de protocole OSPFv3, à la page 981
- Supervision OSPF, à la page 982
- Historique OSPF, à la page 984

Routage OSPF

OSPF est un protocole de routage de passerelle intérieure qui

- utilise des états de liaison plutôt que des vecteurs de distance pour la sélection de chemin,
- propage des annonces d'état de liaison plutôt que des mises à jour de la table de routage, et
- converge plus rapidement que les réseaux RIP parce que seuls les LSA sont échangés au lieu des tableaux de routage complets.

Fonctionnalités et caractéristiques d'OSPF

OSPF utilise un algorithme d'état de liens pour créer et calculer le chemin le plus court vers toutes les destinations connues. Chaque routeur d'une zone OSPF contient une base de données d'états de liaison identique, qui est une liste de chacune des interfaces utilisables et des voisins accessibles du routeur.

Les avantages d'OSPF par rapport à RIP comprennent les caractéristiques suivantes :

- Les mises à jour de la base de données d'états de liens OSPF sont envoyées moins fréquemment que les mises à jour RIP, et la base de données d'états de liens est mise à jour instantanément, plutôt que lentement, à mesure que les informations périmées expirent.

- Les décisions de routage sont basées sur le coût, qui est une indication du surdébit nécessaire pour envoyer des paquets sur une certaine interface. ASA calcule le coût d'une interface en fonction de la bande passante du lien plutôt que du nombre de sauts vers la destination. Le coût peut être configuré pour préciser les chemins privilégiés.

L'inconvénient des algorithmes du chemin le plus court d'abord est qu'ils nécessitent beaucoup de cycles du processeur et de mémoire.

L'ASA peut exécuter deux processus du protocole OSPF simultanément sur différents ensembles d'interfaces. Vous pourriez souhaiter exécuter deux processus si vous avez des interfaces qui utilisent les mêmes adresses IP (la NAT permet à ces interfaces de coexister, mais OSPF ne permet pas le chevauchement d'adresses). Ou vous pouvez exécuter un processus à l'intérieur et un autre à l'extérieur et redistribuer un sous-ensemble de routes entre les deux processus. De même, vous devrez peut-être séparer les adresses privées des adresses publiques.

Vous pouvez redistribuer les routages dans un processus de routage OSPF à partir d'un autre processus de routage OSPF, d'un processus de routage IP ou de routes statiques et connectées configurées sur des interfaces activées pour OSPF.

L'ASA prend en charge les fonctionnalités OSPF suivantes :

- Routages intra-zones, inter-zones et externes (type I et type II).
- Liens virtuels.
- Inondation de LSA.
- Authentification pour les paquets OSPF (authentification par mot de passe et authentification MD5).
- Configuration de l'ASA en tant que routeur désigné ou routeur de secours désigné. L'ASA peut également être configuré comme un ABR.
- Zones tampons et zones tampons.
- Routeur de frontière de zone, filtrage LSA de type 3

OSPF prend en charge MD5 et l'authentification du voisin en texte clair. L'authentification doit être utilisée avec tous les protocoles de routage lorsque cela est possible, car la redistribution de routage entre OSPF et d'autres protocoles (comme RIP) peut être utilisée par des agresseurs pour détourner les informations de routage.

Si la NAT est utilisée, si OSPF fonctionne sur des zones publiques et privées, et si le filtrage d'adresses est requis, vous devez exécuter deux processus OSPF, un pour les zones publiques et un pour les zones privées.

Un routeur qui a des interfaces dans plusieurs zones est appelé routeur de frontière de zone (ABR). Un routeur qui agit comme une passerelle pour redistribuer le trafic entre les routeurs utilisant OSPF et les routeurs utilisant d'autres protocoles de routage est appelé un routeur de frontière de système autonome (ASBR).

Un ABR utilise des LSA pour envoyer des informations sur les routes disponibles à d'autres routeurs OSPF. Le filtrage des LSA de type 3 d'un ABR vous permet de disposer de zones privées et publiques distinctes, l'ASA agissant comme ABR. Les LSA de type 3 (routes inter-zones) peuvent être filtrées d'une zone à une autre, ce qui vous permet d'utiliser la NAT et l'OSPF ensemble sans annoncer de réseaux privés.

Remarque Seuls les LSA de type 3 peuvent être filtrés. Si vous configurez l'ASA comme ASBR dans un réseau privé, il enverra des LSA de type 5 décrivant les réseaux privés, qui seront inondés à l'ensemble du système autonome, y compris les zones publiques.

Si la NAT est utilisée, mais qu'OSPF s'exécute uniquement dans les zones publiques, les routes vers les réseaux publics peuvent être redistribuées dans le réseau privé, soit par défaut, soit sous forme de LSA externes de type 5. Cependant, vous devez configurer des routes statiques pour les réseaux privés protégés par ASA. De plus, vous ne devez pas combiner réseaux publics et réseaux privés sur la même interface ASA.

Vous pouvez avoir deux processus de routage OSPF, un processus de routage RIP et un processus de routage EIGRP en même temps sur l'ASA.

Prise en charge OSPF pour les paquets Fast Hello

La prise en charge OSPF pour les paquets Fast Hello

- permet de configurer l'envoi de paquets Hello par intervalles inférieurs à une seconde, et
- entraîne une convergence plus rapide dans un réseau OSPF (Open Shortest Path First).

Conditions préalables à la configuration des paquets Hello rapide d'OSPF

OSPF doit déjà être configuré dans le réseau ou configuré en même temps que la fonction de prise en charge OSPF des paquets Fast Hello.

À propos de la prise en charge OSPF pour les paquets Hello rapides

Les concepts clés liés à la prise en charge OSPF pour les paquets Fast Hello et aux avantages des paquets OSPF Fast Hello sont décrits ci-dessous :

Intervalle Hello et intervalle mort OSPF

L'intervalle Hello et l'intervalle mort d'OSPF sont des paramètres de temps configurables qui

- maintiennent la connectivité entre les voisins OSPF par des échanges réguliers de paquets Hello,
- détectent les défaillances de voisins lorsque les paquets Hello ne sont pas reçus dans les délais spécifiés, et
- doivent être cohérents sur tous les routeurs d'un même réseau pour assurer un fonctionnement adéquat.

Détails de la configuration des intervalles Hello et des intervalles morts

Les paquets Hello OSPF sont des paquets qu'un processus OSPF envoie à ses voisins OSPF pour maintenir la connectivité avec ces derniers. Les paquets Hello sont envoyés à un intervalle configurable (en secondes). Les valeurs par défaut sont de 10 secondes pour une liaison Ethernet et de 30 secondes pour une liaison non diffusée.

Les paquets Hello comprennent une liste de tous les voisins pour lesquels un paquet Hello a été reçu dans l'intervalle mort. L'intervalle mort est également un intervalle configurable (en secondes). Par défaut, il est

quatre fois supérieur à la valeur de l'intervalle Hello. La valeur de tous les intervalles Hello doit être la même dans un réseau. De même, la valeur de tous les intervalles morts doit être la même dans un réseau.

Ces deux intervalles fonctionnent ensemble pour maintenir la connectivité en indiquant que la liaison est opérationnelle. Si un routeur ne reçoit pas de paquet Hello d'un voisin dans l'intervalle mort, il déclarera ce voisin en panne.

Paquets Hello rapides OSPF

Les paquets Hello rapides d'OSPF sont des paquets Hello qui

- sont envoyés à des intervalles inférieurs à 1 seconde,
- sont obtenus à l'aide de la commande OSPF dead-interval avec un intervalle d'inactivité défini à 1 seconde, et
- utilisent une valeur de multiplicateur Hello définie sur le nombre de paquets Hello envoyés pendant cette seconde.

Comportement des paquets Hello rapides

Lorsque des paquets Hello rapides sont configurés sur l'interface, ces comportements se produisent :

- L'intervalle Hello annoncé dans les paquets Hello envoyés par cette interface est réglé à 0.
- L'intervalle Hello dans les paquets Hello reçus sur cette interface est ignoré.

L'intervalle mort doit être cohérent sur un segment, qu'il soit défini à 1 seconde (pour les paquets Hello rapides) ou à une autre valeur. Le multiplicateur Hello n'a pas besoin d'être le même pour tout le segment tant qu'au moins un paquet Hello est envoyé dans l'intervalle mort.

Pour comprendre les paquets Hello rapides, vous devez déjà comprendre la relation entre les paquets Hello d'OSPF et l'intervalle mort. Consultez Intervalle Hello et intervalle mort OSPF, à la page 933.

Avantages des paquets Hello rapides OSPF

Un paquet Hello rapide est une fonctionnalité du protocole OSPF qui

- réduit le temps de convergence du réseau en permettant aux routeurs de détecter plus rapidement les modifications dans le réseau,
- permet la détection rapide des voisins perdus en une seconde, et
- améliore la fiabilité dans les environnements LAN où la perte de voisin peut ne pas être détectée au niveau de la couche physique ou de la couche liaison de données de l'Open Systems Interconnection (OSI).

L'intérêt des paquets Hello rapides OSPF est que votre réseau OSPF peut réagir rapidement aux modifications, ce qui réduit les temps d'arrêt et améliore la stabilité globale du réseau. Cette fonctionnalité est particulièrement utile dans les scénarios où les routeurs ne peuvent pas détecter les voisins perdus par les méthodes traditionnelles, ce qui permet à OSPF de maintenir des tables de routage précises.

Si un routeur sur un segment de réseau local (LAN) est hors tension ou déconnecté et que les couches physique et liaison de données ne signalent pas la perte du voisin, les paquets Hello rapides OSPF détecteront la disparition du voisin en une seconde.

Différences d'implémentation entre OSPFv2 et OSPFv3

Une distinction de protocole est une catégorie de protocole qui

- empêche la rétrocompatibilité entre OSPFv2 et OSPFv3,
- nécessite que les deux versions d'OSPF fonctionnent simultanément pour le routage IPv4 et IPv6, et
- permet à OSPFv2 et OSPFv3 de coexister sans interagir l'un avec l'autre.

Fonctionnalités supplémentaires d'OSPFv3

Les fonctionnalités supplémentaires fournies par OSPFv3 sont les suivantes :

- Traitement du protocole par liaison
- Suppression de la sémantique d'adressage.
- Ajout de la portée de submersion.
- Prise en charge de plusieurs instances par lien.
- Utilisation de l'adresse locale de lien IPv6 pour la découverte de voisin et d'autres fonctionnalités.
- Les LSA sont exprimées en tant que préfixe et longueur de préfixe.
- Ajout de deux types de LSA.
- Gestion des types de LSA inconnus
- Prise en charge de l'authentification par la norme IPsec ESP pour le trafic de protocole de routage OSPFv3, comme le spécifie la RFC 4552.

Directives pour OSPF

Lignes directrices relatives au mode contextuel

OSPFv2 prend en charge les modes à contexte unique et multiple.

- Les instances OSPFv2 ne peuvent pas former de contiguïtés entre elles dans les interfaces partagées car, par défaut, l'échange inter-contextes du trafic de multidiffusion n'est pas pris en charge sur les interfaces partagées. Cependant, vous pouvez utiliser la configuration de voisin statique sous la configuration de processus OSPFv2 sous le processus OSPFv2 pour faire apparaître le voisinage OSPFv2 sur une interface partagée.
- OSPFv2 inter-contexte sur des interfaces distinctes est pris en charge.
- **(Pour la topologie point à point)** En mode de contexte multiple, vous pouvez configurer des voisins OSPFv2 statiques pour annoncer les routes OSPFv2 sur un réseau point à point de non-diffusion. Pour une formation réussie de l'adjacence OSPF, lorsque vous supprimez et reconfigurez OSPF sur une interface partagée, exécutez les commandes dans cet ordre : supprimez la configuration OSPF à l'aide de **no router <OSPF name>**, puis retirez la configuration OSPF point à point sans diffusion sur l'interface à l'aide de **no OSPF network point-to-point non-broadcast**. Lorsque vous reconfigurez OSPF sur l'interface partagée, configurez le routeur OSPF en utilisant **router <OSPF name>**, puis configurez l'interface avec **OSPF network point-to-point non-broadcast**.

- OSPFv3 prend en charge le mode unique uniquement.

Lignes directrices d'authentification par chaîne de clé

OSPFv2 prend en charge l'authentification par chaîne de clés en mode unique et multiple, en modes physique et virtuel. Cependant, en mode multiple, vous pouvez configurer la chaîne de clés uniquement en mode contextuel.

- Les clés pivotantes ne s'appliquent qu'au protocole OSPFv2. L'authentification de zone OSPF avec chaîne de clé n'est pas prise en charge.
- L'authentification MD5 existante sans plage temporelle dans OSPFv2 est toujours prise en charge avec les nouvelles clés alternées.
- Bien que la plateforme prenne en charge les algorithmes cryptographiques SHA1 et MD5, seul l'algorithme cryptographique MD5 est utilisé pour l'authentification.

Lignes directrices sur le mode pare-feu

OSPF ne prend en charge que le mode pare-feu routé. OSPF ne prend pas en charge le mode de pare-feu transparent.

Directives Basculement

OSPFv2 et OSPFv3 prennent en charge le Basculement sans état.

Lignes directrices IPv6

OSPFv2 ne prend pas en charge IPv6, tandis qu'OSPFv3 fournit une prise en charge d'IPv6 avec des capacités d'authentification et de routage spécifiques.

- OSPFv2 ne prend pas en charge IPv6.
- OSPFv3 prend en charge IPv6.
- OSPFv3 utilise IPv6 pour l'authentification.
- L'ASA installe les routages OSPFv3 dans le RIB IPv6, à condition qu'il s'agisse du meilleur routage.
- Les paquets OSPFv3 peuvent être filtrés à l'aide des listes de contrôle d'accès IPv6 dans la commande **capture**.

Paquets Hello OSPFv3 et GRE

En règle générale, le trafic OSPF ne passe pas par le tunnel GRE. Lorsqu'OSPFv3 sur IPv6 est encapsulé à l'intérieur de GRE, la validation de l'en-tête IPv6 pour les vérifications de sécurité telles que la destination de multidiffusion échoue. Le paquet est abandonné en raison de la validation de vérification de sécurité implicite, car ce paquet a une multidiffusion IPv6 de destination.

- Vous pouvez définir une règle de préfiltre pour contourner le trafic GRE. Cependant, avec la règle de préfiltre, les paquets internes ne seraient pas interrogés par le moteur d'inspection.

Lignes directrices de mise en grappe

OSPFv2 et OSPFv3 ont des limites et des comportements spécifiques dans les environnements de mise en grappe.

- Le chiffrement OSPFv3 n'est pas pris en charge. Un message d'erreur s'affiche si vous essayez de configurer le chiffrement OSPFv3 dans un environnement de mise en grappe.
- En mode d'interface étendue, le routage dynamique n'est pas pris en charge sur les interfaces de gestion uniquement.
- En mode d'interface individuel, veillez à définir les unités de contrôle et de données comme des voisins OSPFv2 ou OSPFv3.
- En mode d'interface individuelle, les contiguïtés OSPFv2 ne peuvent être établies qu'entre deux contextes sur une interface partagée sur l'unité de contrôle. La configuration de voisins statiques est prise en charge uniquement sur les liaisons point à point; par conséquent, une seule instruction voisin est autorisée sur une interface.
- Lorsqu'un changement de rôle de contrôle se produit dans la grappe, un comportement spécifique se produit en fonction du mode d'interface. En mode d'interface étendue, le processus du routeur est actif uniquement sur l'unité de contrôle et est à l'état suspendu sur les unités de données. Chaque unité de grappe a le même ID de routeur, car la configuration a été synchronisée à partir de l'unité de contrôle. Par conséquent, un routeur voisin ne remarque aucun changement dans l'ID de routeur de la grappe lors d'un changement de rôle. En mode d'interface individuelle, le processus du routeur est actif sur toutes les unités de la grappe. Chaque unité de grappe choisit son propre ID de routeur dans l'ensemble de grappes configuré. Une modification du rôle de contrôle dans la grappe ne modifie en rien la topologie de routage.

Commutation multiprotocole par étiquette (MPLS) et Lignes directrices OSPF

Lorsqu'un routeur configuré pour MPLS envoie des paquets de mise à jour d'état de liaison (LS) qui contiennent des publicités d'état de liaison (LSA) de type 10 couvrantes qui comprennent un en-tête MPLS, l'authentification échoue et le périphérique abandonne en mode silencieux les paquets de mise à jour plutôt que d'en accuser réception. Finalement, le routeur homologue mettra fin à la relation de voisin, car il n'a reçu aucun accusé de réception.

- Désactivez la capacité d'opacité sur l'ASA pour vous assurer que la relation de voisin reste stable :

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```

Ces lignes directrices s'appliquent aux environnements MPLS dans lesquels les LSA opaques peuvent entraîner des échecs d'authentification.

Remarque Les modèles Firepower 4100/9300 peuvent avoir une latence élevée lors de l'utilisation de MPLS, car ils n'ont pas suffisamment d'équilibrage de la charge sur plusieurs files d'attente de réception.

Lignes directrices relatives à la redistribution des voies de routage

La redistribution des voies de routage avec des listes de préfixes et entre les domaines de routage nécessite des considérations de configuration spécifiques.

- La redistribution des cartes de routage avec la liste de préfixes IPv4 sur OSPFv2 est prise en charge. Toutefois, la redistribution des cartes de routage avec la liste de préfixes IPv6 sur OSPFv3 n'est pas prise en charge. Utilisez une liste d'accès dans la carte de routage sur OSPF pour la redistribution.

- Lorsqu'OSPF est configuré sur un périphérique qui fait partie du réseau EIGRP ou inversement, assurez-vous que le routeur OSPF est configuré pour baliser la voie de routage (le protocole EIGRP ne prend pas encore en charge la balise de routage). Lors de la redistribution d'OSPF dans EIGRP et d'EIGRP dans OSPF, une boucle de routage se produit lorsqu'il y a une panne sur l'une des liaisons ou des interfaces ou même lorsque l'expéditeur de la route est en panne. Pour empêcher la redistribution des routages d'un domaine vers le même domaine, un routeur peut marquer un routage qui appartient à un domaine pendant qu'il redistribue, et ces routages peuvent être filtrés sur le routeur distant en se basant sur la même balise. Comme les routes ne seront pas installées dans la table de routage, elles ne seront pas redistribuées dans le même domaine.

Lignes directrices supplémentaires

OSPFv2 et OSPFv3 prennent en charge diverses fonctionnalités et ont des limites spécifiques dans différents scénarios de déploiement.

- OSPFv2 et OSPFv3 prennent en charge plusieurs instances sur une interface.
- OSPFv3 prend en charge le chiffrement par le biais des en-têtes ESP dans un environnement sans grappe.
- OSPFv3 prend en charge le chiffrement sans charge utile.
- OSPFv2 prend en charge les mécanismes de redémarrages progressifs NSF de Cisco et IETF NSF tels que définis dans les RFC 4811, 4812 et 3623 respectivement.
- OSPFv3 prend en charge le mécanisme de redémarrage progressif tel que défini dans la RFC 5187.
- Il y a une limite au nombre de routages intra-zone (type 1) qui peuvent être distribués. Pour ces routes, un seul LSA de type 1 contient tous les préfixes. Comme le système a une limite de 35 Ko pour la taille des paquets, un paquet de 3 000 routages dépasse la limite. Considérez 2900 routes de type 1 comme le nombre maximal pris en charge.
- Pour éviter les oscillations de contiguïté dues aux mises à jour de routage abandonnées si la mise à jour de routage est supérieure à la MTU minimale sur le lien, configurez la même MTU sur les interfaces des deux côtés du lien.
- L'ASA virtuel ne peut pas utiliser les protocoles de routage interne dynamique comme EIGRP et OSPF en raison de la nature du routage dans le nuage Azure. La table de routage effective détermine le saut suivant, que le client virtuel ait ou non une route statique/dynamique configurée. Actuellement, vous ne pouvez pas afficher la table de routage effective ou la table de routage du système.
- OSPFv3 abandonne la mise à jour LS si la taille des paquets dépasse 8190. Par conséquent, le voisinage est interrompu. Ainsi, configurez le commutateur avec la commande « ospfv3 MTU-ignore » pour éviter la fin du voisinage.

Configurer le protocole OSPFv2

Cette section décrit comment activer un processus OSPFv2 sur l'ASA.

Après avoir activé le protocole OSPFv2, vous devez définir une carte de routage. Pour en savoir plus, consultez Définir une carte de routage, à la page 885. Ensuite, vous générez une route par défaut. Pour en savoir plus, consultez Configurer une route statique, à la page 867.

Après avoir défini une carte de routage pour le processus OSPFv2, vous pouvez la personnaliser selon vos besoins particuliers. Pour savoir comment personnaliser le processus OSPFv2 sur l'ASA, consultez Personnaliser le protocole OSPFv2, à la page 943.

Pour activer le protocole OSPFv2, vous devez créer un processus de routage OSPFv2, spécifier la plage d'adresses IP associées au processus de routage, puis attribuer les ID de zone associés à cette plage d'adresses IP.

Vous pouvez activer jusqu'à deux instances de processus OSPFv2. Chaque processus OSPFv2 a ses propres zones et réseaux associés.

Pour activer le processus OSPFv2, procédez comme suit.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Dans le volet OSPF Setup (Configuration du protocole OSPF), vous pouvez activer les processus OSPF, configurer les zones et les réseaux OSPF, et définir la synthèse des routes OSPF.

Étape 2 Les trois onglets dans ASDM utilisés pour activer OSPF sont les suivants :

- L'onglet Process Instances (Instances de processus) vous permet d'activer jusqu'à deux instances de processus OSPF pour chaque contexte. Le mode de contexte unique et le mode de contexte multiple sont tous deux pris en charge. Après avoir coché la case **Enable Each OSPF Process** (Activer chaque processus OSPF), vous pouvez saisir un identifiant numérique unique pour ce processus OSPF. Cet ID de processus est utilisé en interne et n'a pas besoin de correspondre à l'ID de processus OSPF sur d'autres appareils OSPF; les valeurs valides sont comprises entre 1 et 65535. Chaque processus OSPF a ses propres zones et réseaux associés.

  Si vous cliquez sur **Advanced** (Avancé), la boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF) apparaît. À partir de là, vous pouvez configurer l'ID de routeur, les réserves d'adresses IP de la grappe dans la mise en grappe de l'interface individuelle ou de l'EtherChannel étendu, les modifications de contiguïté, les distances de route administratives, les minuteries et les paramètres d'origine des renseignements par défaut pour chaque processus OSPF. .

- L'onglet Area/Networks (Zone/Réseaux) vous permet d'afficher les zones et les réseaux qu'elles incluent pour chaque processus OSPF sur l'ASA. À partir de cet onglet, vous pouvez afficher l'ID de zone, le type de zone et le type d'authentification défini pour la zone. Pour ajouter ou modifier une zone ou un réseau OSPF, consultez Configurer les paramètres de zone OSPFv2, à la page 951 pour de plus amples renseignements.

- L'onglet Route Summarization (Synthèse des routes) vous permet de configurer un ABR. Dans OSPF, un ABR annoncera des réseaux d'une zone dans une autre zone. Si les numéros de réseau d'une zone sont affectés de manière à ce qu'ils soient contigus, vous pouvez configurer l'ABR pour annoncer une route récapitulative qui inclut tous les réseaux individuels de la zone qui entrent dans la plage spécifiée. Consultez Configurer la synthèse des routes entre les zones OSPFv2, à la page 947 pour de plus amples renseignements.

Configurer une chaîne de clés pour l'authentification

Pour améliorer la sécurité et la protection des données des périphériques, vous pouvez activer des clés changeantes pour l'authentification des homologues IGP. Les clés pivotantes empêchent tout utilisateur malveillant de deviner les clés utilisées pour l'authentification du protocole de routage, protégeant ainsi le réseau contre les annonces de routage incorrect et la redirection du trafic. La modification fréquente des clés réduit le risque qu'elles finissent par être devinées. Lors de la configuration de l'authentification pour les protocoles de routage qui fournissent des chaînes de clés, configurez les clés d'une chaîne de clés pour qu'elles se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active. Si la durée de vie de la clé expire et qu'aucune clé active n'est trouvée, OSPF utilise la dernière clé valide pour maintenir la contiguïté avec les homologues.

Cette section décrit comment créer une chaîne de clés pour l'authentification des homologues OSPF. Cette section couvre également les étapes pour ajouter ou modifier les attributs d'une chaîne de clés. Après avoir configuré un objet de chaîne de clés, vous pouvez l'utiliser pour définir l'authentification OSPFv2 pour une interface et pour une liaison virtuelle. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie. Pour savoir comment définir l'authentification pour une interface, consultez Configurer les paramètres d'interface OSPFv2, à la page 947; pour une liaison virtuelle, consultez Configurer un lien virtuel dans OSPF, à la page 961.

Pour configurer une chaîne de clés, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Key Chain (Chaîne de clés)** .

Étape 2 Dans la section **Configure Key Chain** (Configurer la chaîne de clés), cliquez sur **Add** (Ajouter).

Étape 3 Saisissez le nom de la chaîne de clés dans la boîte de dialogue **Add Key Chain** (Ajouter une chaîne de clés), puis cliquez sur **OK**.

Le nom de la chaîne de clés créée est répertorié dans la grille **Configure Key Chain** (Configurer la chaîne de clés).

Étape 4 Sélectionnez le nom de la chaîne de clés dans la section **Configure Key Chain** (Configurer la chaîne de clés), et dans la section **Configure Key** (Configurer la clé), cliquez sur **Add** (Ajouter). Pour modifier une clé existante, sélectionnez le nom de la clé et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Add Key** (Ajouter une clé) ou **Edit Key** (Modifier une clé) apparaît, selon l'action que vous avez sélectionnée.

Étape 5 Précisez l'identifiant de clé dans le champ **Key ID**.

La valeur de l'ID de clé peut être comprise entre 0 et 255. Utilisez la valeur 0 uniquement lorsque vous souhaitez signaler une clé non valide.

Remarque Vous ne pouvez pas modifier un ID de clé enregistré.

Étape 6 Dans la liste déroulante **Cryptographic Algorithm** (Algorithme cryptographique), choisissez **MD5**. MD5 est le seul algorithme pris en charge pour l'authentification de la chaîne de clés.

Étape 7 Sélectionnez le type de chiffrement en cliquant sur le bouton radio **Plain Text** (Texte brut) ou **Encrypted** (Chiffré), puis saisissez le mot de passe dans le champ **Authentication Key** (Clé d'authentification).

- Même si la chaîne de clé peut contenir 80 caractères, seul un maximum de 64 caractères est autorisé pour l'authentification OSPF.
- Les mots de passe ne peuvent pas être un seul chiffre ni ceux commençant par un chiffre suivi d'un espace. Par exemple, « 0 pass » ou « 1 » ne sont pas valides.

Étape 8 Fournissez les valeurs de durée de vie dans les champs **Accept Lifetime** (Accepter la durée de vie) et **Send Lifetime** (Envoyer la durée de vie) :

Vous pouvez spécifier l'intervalle de temps nécessaire pour que le périphérique accepte ou envoie la clé lors de l'échange de clés avec un autre périphérique. L'heure de fin peut correspondre à la durée absolue à laquelle la durée de vie de l'acceptation/envoi se termine ou n'expire jamais.

Voici les règles de validation pour les valeurs de début et de fin :

- La durée de vie de début ne peut pas être nulle lorsque la fin de vie est spécifiée.
- La durée de vie de début pour l'acceptation ou l'envoi de la durée de vie doit être antérieure à la fin de vie.

Étape 9 Pour enregistrer les attributs de la chaîne de clés, cliquez sur **OK**. Dans la page **Key Chain** (Chaîne de clés), cliquez sur **Appy** (Appliquer).

Prochaine étape

Vous pouvez maintenant appliquer la chaîne de clés configurée pour définir l'authentification OSPFv2 pour une interface et pour la liaison virtuelle.

- Configurer les paramètres d'interface OSPFv2, à la page 947
- Configurer un lien virtuel dans OSPF, à la page 961

Configurer l'ID de routeur OSPFv2

L'ID de routeur OSPF est utilisé pour identifier un appareil spécifique dans une base de données OSPF. Deux routeurs d'un système OSPF ne peuvent pas avoir le même ID de routeur.

Si un ID de routeur n'est pas configuré manuellement dans le processus de routage OSPF, le routeur configurera automatiquement un ID de routeur déterminé à partir de l'adresse IP la plus élevée d'une interface active. Lors de la configuration d'un ID de routeur, les voisins ne seront pas mis à jour automatiquement jusqu'à ce que le routeur ait échoué ou que le processus OSPF ait été effacé et que la relation de voisin ait été rétablie.

Configurer manuellement l'ID de routeur OSPF

Cette section décrit comment configurer manuellement l'ID de routeur dans le processus OSPFv2 sur l'ASA.

Procédure

Étape 1 Pour utiliser un ID de routeur fixe, utilisez la commande **router-id**.

router-id *ip-address*

Exemple :

```
ciscoasa(config-router)# router-id 193.168.3.3
```

Étape 2 Pour revenir au comportement précédent de l'ID de routeur OSPF, utilisez la commande **no router-id**.

no router-id *ip-address*

Exemple :

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

Comportement de l'ID de routeur lors de la migration

Lors de la migration de la configuration OSPF d'un ASA, par exemple ASA 1 vers un autre ASA, par exemple l'ASA 2, le comportement suivant est observé en matière de sélection de l'ID du routeur :

1. L'ASA 2 n'utilise aucune adresse IP pour l'ID de routeur OSPF lorsque toutes les interfaces sont en mode d'arrêt. Les possibilités de configuration de l'ID de routeur lorsque toutes les interfaces sont à l'état « arrêt admin » ou en mode d'arrêt sont les suivantes :
   - Si l'ASA 2 n'a pas encore d'ID de routeur configuré, vous verrez ce message :

     `%OSPF: Router process 1 is not running, please configure a router-id` (% OSPF : le processus de routeur 1 n'est pas en cours d'exécution, veuillez configurer un identifiant de routeur)

     Après le déploiement de la première interface, l'ASA 2 utilisera l'adresse IP de cette interface comme ID de routeur.
   - Si l'ASA 2 a déjà configuré l'ID de routeur et que toutes les interfaces étaient à l'état « arrêt admin » lorsque la commande « no router-id » a été exécutée, l'ASA 2 utilisera l'ancien ID de routeur. L'ASA 2 utilise l'ancien ID de routeur, même si les adresses IP de l'interface créée sont modifiées, jusqu'à ce que la commande « clear ospf process » soit émise.
2. L'ASA 2 utilise un nouvel ID de routeur, alors que l'ASA 2 avait déjà configuré l'ID de routeur et qu'au moins une des interfaces n'était pas à l'état « arrêt admin » ou en mode d'arrêt lorsque la commande « no router-id » a été émise. L'ASA 2 utilisera le nouvel ID de routeur de l'adresse IP des interfaces même lorsque les interfaces sont à l'état « arrêt/arrêt ».

Personnaliser le protocole OSPFv2

Cette section explique comment personnaliser les processus OSPFv2.

Redistribuer les routes dans OSPFv2

L'ASA peut contrôler la redistribution des routes entre les processus de routage OSPFv2.

Remarque Si vous souhaitez redistribuer une route en définissant quelles routes du protocole de routage spécifié peuvent être redistribuées dans le processus de routage cible, vous devez d'abord générer une route par défaut. Consultez Configurer une route statique, à la page 867, puis définissez une carte de routage en fonction de Définir une carte de routage, à la page 885.

Pour redistribuer les routes statiques, connectées, RIP ou OSPFv2 dans un processus OSPFv2, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Redistribution**.

Le volet Redistribution affiche les règles de redistribution des routes d'un processus de routage vers un processus de routage OSPF. Vous pouvez redistribuer les routes détectées par RIP et OSPF dans le processus de routage EIGRP. Vous pouvez également redistribuer les routes statiques et connectées dans le processus de routage EIGRP. Vous n'avez pas besoin de redistribuer les routes statiques ou connectées si elles entrent dans la plage d'un réseau qui a été configuré par le biais de l'onglet Setup (Configurer) > Networks (Réseaux).

Étape 2 Cliquez sur **Add** ou **Edit** (ajouter ou modifier).

Sinon, le double-clic sur une entrée de tableau dans le volet Redistribution (le cas échéant) ouvre la boîte de dialogue Add/Edit OSPF Redistribution Entry (Ajouter/modifier une entrée de redistribution OSPF) pour l'entrée sélectionnée.

Remarque Toutes les étapes suivantes sont facultatives.

La boîte de dialogue Add/Edit OSPF Redistribution Entry (Ajouter/modifier une entrée de redistribution OSPF) vous permet d'ajouter une nouvelle règle de redistribution ou de modifier une règle de redistribution existante dans le tableau de redistribution. Certaines informations sur la règle de redistribution ne peuvent pas être modifiées lorsque vous modifiez une règle de redistribution existante.

Étape 3 Choisissez le processus OSPF associé à l'entrée de redistribution des routes. Si vous modifiez une règle de redistribution existante, vous ne pouvez pas modifier ce paramètre.

Étape 4 Choisissez le protocole source à partir duquel les routes sont redistribuées. Vous pouvez choisir l'une des options suivantes :

- Static (statique) : redistribue les routes statiques vers le processus de routage OSPF.
- Connected (Connecté) : redistribue les routes connectées (les routes sont établies automatiquement parce que l'adresse IP est activée sur l'interface) vers le processus de routage OSPF. Les routes connectées sont redistribuées en tant que routes externes vers l'AS.
- OSPF : redistribue les routes à partir d'un autre processus de routage OSPF. Choisissez l'ID de processus OSPF dans la liste. Si vous choisissez ce protocole, les options de correspondance de cette boîte de dialogue deviennent visibles. Ces options ne sont pas disponibles lors de la redistribution de routes statiques, connectées, RIP ou EIGRP. Passez à l'étape 5.
- RIP : redistribue les routes à partir du processus de routage RIP.
- BGP : redistribue les routes à partir du processus de routage BGP.
- EIGRP : redistribue les routes à partir du processus de routage EIGRP. Choisissez le numéro de système autonome du processus de routage EIGRP dans la liste.

Étape 5 Si vous avez choisi OSPF pour le protocole source, choisissez les conditions utilisées pour la redistribution des routes d'un autre processus de routage OSPF dans le processus de routage OSPF sélectionné. Ces options ne sont pas disponibles lors de la redistribution de routes statiques, connectées, RIP ou EIGRP. Les routages doivent correspondre à la condition sélectionnée pour être redistribués. Vous pouvez choisir une ou plusieurs des conditions de correspondance suivantes :

- Internal (Interne) : la route est interne à un AS spécifique.
- External 1 (Externe 1) : les routes sont externes au système autonome, mais importées dans OSPF en tant que routes externes de type 1.
- External 2 (Externe 2) : les routes sont externes au système autonome, mais importées dans OSPF en tant que routes externes de type 2.
- NSSA External 1 (NSSA Externe 1) : les routes sont externes au système autonome, mais importées dans OSPF en tant que routes externes NSSA de type 1.
- NSSA External 2 (NSSA Externe 2) : les routes sont externes au système autonome, mais importées dans OSPF en tant que routes externes NSSA de type 2.

Étape 6 Dans le champ **Metric Value** (Valeur de la mesure), saisissez la valeur de la mesure pour les routes redistribuées. Les valeurs valides sont comprises entre 1 et 16777214.

Lors de la redistribution d'un processus OSPF à un autre processus OSPF sur le même périphérique, la mesure sera transmise d'un processus à l'autre si aucune valeur de mesure n'est spécifiée. Lors de la redistribution d'autres processus vers un processus OSPF, la mesure par défaut est 20 lorsqu'aucune valeur de mesure n'est spécifiée.

Remarque La redistribution des routes statiques avec une carte de routage correspondant à une mesure n'est pas prise en charge.

Étape 7 Choisissez l'une des options suivantes pour le type de mesure.

- Si la mesure est une route externe de type 1, choisissez **1**.
- Si la mesure est une route externe de type 2, choisissez **2**.

Étape 8 Saisissez la valeur de la balise dans le champ **Tag Value** (Valeur de balise).

La valeur de la balise est une valeur décimale sur 32 bits associée à chaque route externe qui n'est pas utilisée par OSPF lui-même, mais qui peut être utilisée pour communiquer des informations entre ASBR. Les valeurs valides vont de 0 à 4294967295.

Étape 9 Cochez la case **Use Subnets** (Utiliser les sous-réseaux) pour activer la redistribution des routes divisées en sous-réseaux. Décochez cette case pour que seules les routes qui ne sont pas divisées en sous-réseaux soient redistribuées.

Étape 10 Choisissez le nom de la carte de routage à appliquer à l'entrée de redistribution dans la liste déroulante Route Map (Carte de routage).

Étape 11 Si vous devez ajouter ou configurer une carte de routage, cliquez sur **Manage** (Gérer).

La boîte de dialogue Configure Route Map (Configurer la carte de routage) apparaît.

Étape 12 Cliquez **Add** (Ajouter) ou **Edit** (Modifier) pour définir les routes du protocole de routage spécifié qui peuvent être redistribuées dans le processus de routage cible. Pour en savoir plus, consultez Définir une carte de routage, à la page 885.

Étape 13 Cliquez sur **OK**.

Configurer la synthèse des routes lors de la redistribution des routes dans OSPFv2

Lorsque les routages d'autres protocoles sont redistribués dans OSPF, chaque routage est annoncée individuellement dans un LSA externe. Cependant, vous pouvez configurer l'ASA pour annoncer une seule route pour toutes les routes redistribuées qui sont incluses pour une adresse et un masque réseau spécifiés. Cette configuration diminue la taille de la base de données d'états de liaison OSPF.

Les routes qui correspondent à la paire de masques d'adresses IP spécifiées peuvent être supprimées. La valeur de balise peut être utilisée comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage.

Ajouter une adresse sommaire de route

Le volet Summary Address (Adresse sommaire) affiche des renseignements sur les adresses sommaires configurées pour chaque processus de routage OSPF.

Les routes apprises d'autres protocoles de routage peuvent être résumées. La métrique utilisée pour annoncer le résumé est la plus petite de toutes les routes spécifiques. Les routages récapitulatifs permettent de réduire la taille de la table de routage.

L'utilisation des routages récapitulatifs pour OSPF amène un ASBR OSPF à annoncer une route externe en tant qu'agrégat pour toutes les routes redistribuées qui sont couvertes par l'adresse. Seuls les routages d'autres protocoles de routage qui sont redistribués dans OSPF peuvent être résumés.



Remarque OSPF ne prend pas en charge l'adresse récapitulative 0.0.0.0 0.0.0.0.

Pour configurer l'annonce du logiciel sur une route récapitulative pour toutes les routes redistribuées incluses pour une adresse réseau et un masque, procédez comme suit :

Procédure

Étape 1 Dans la page d'accueil principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Summary Address (Adresse sommaire)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue Add OSPF Summary Address Entry (Ajouter une entrée d'adresse sommaire OSPF) s'affiche. Vous pouvez ajouter de nouvelles entrées aux entrées existantes dans le tableau d'adresses sommaires. Certains renseignements sur les adresses sommaires ne peuvent pas être modifiés lors de la modification d'une entrée existante.

Étape 3 Choisissez l'ID de processus OSPF spécifié associé à l'adresse sommaire dans la liste déroulante OSPF Process (Processus OSPF). Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 4 Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de l'adresse sommaire. Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 5 Dans la liste déroulante **Netmask** (Masque réseau), choisissez le masque réseau pour l'adresse sommaire. Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 6 Cochez la case **Advertise** (Annoncer) pour annoncer la route récapitulative. Décochez cette case pour supprimer les routages qui relèvent de l'adresse résumée. Par défaut, cette case est cochée.

La valeur Tag (Balise) affiche une valeur décimale de 32 bits associée à chaque route externe. Cette valeur n'est pas utilisée par OSPF lui-même, mais peut être utilisée pour communiquer des informations entre ASBR.

Étape 7 Cliquez sur **OK**.

Ajouter ou modifier une adresse sommaire OSPF

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Route Summarization** (Synthèse de routage).

La boîte de dialogue Add/Edit a Route Summarization Entry (Ajouter/modifier une entrée de synthèse de routage) apparaît.

La boîte de dialogue Add/Edit a Route Summarization Entry (Ajouter/modifier une entrée de synthèse de routage) vous permet d'ajouter de nouvelles entrées ou de modifier les entrées existantes dans le tableau des adresses sommaires. Certains renseignements sur les adresses sommaires ne peuvent pas être modifiés lors de la modification d'une entrée existante.

Étape 3 Choisissez l'ID de processus OSPF spécifié associé à l'adresse sommaire dans la liste déroulante **OSPF Process** (Processus OSPF). Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 4 Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de l'adresse sommaire. Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 5 Dans la liste déroulante **Netmask** (Masque réseau), saisissez le masque réseau pour l'adresse sommaire. Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 6 Cochez la case **Advertise** (Annoncer) pour annoncer la route récapitulative. Décochez cette case pour supprimer les routages qui relèvent de l'adresse résumée. Par défaut, cette case est cochée.

Configurer la synthèse des routes entre les zones OSPFv2

La synthèse du routage est le regroupement d'adresses annoncées. Cette fonctionnalité permet d'annoncer une seule route récapitulative à d'autres zones par un routeur de délimitation de zone. Dans OSPF, un routeur de délimitation de zone annonce les réseaux d'une zone dans une autre zone. Si les numéros de réseau d'une zone sont affectés de manière à ce qu'ils soient contigus, vous pouvez configurer le routeur de délimitation de zone pour annoncer une route récapitulative qui inclut tous les réseaux individuels de la zone qui entrent dans la plage spécifiée.

Pour définir une plage d'adresses pour la synthèse du routage, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Route Summarization** (Synthèse de routage).

La boîte de dialogue Add/Edit a Route Summarization Entry (Ajouter/modifier une entrée de synthèse de routage) apparaît.

La boîte de dialogue Add/Edit a Route Summarization Entry (Ajouter/modifier une entrée de synthèse de routage) vous permet d'ajouter de nouvelles entrées ou de modifier les entrées existantes dans le tableau des adresses sommaires. Certains renseignements sur les adresses sommaires ne peuvent pas être modifiés lors de la modification d'une entrée existante.

Étape 3 Saisissez l'ID de zone OSPF dans le champ **Area ID** (ID de zone). Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 4 Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de l'adresse sommaire. Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Configurer les paramètres d'interface OSPFv2

Vous pouvez modifier certains paramètres OSPFv2 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : l'intervalle Hello, l'intervalle de temps mort et la clé d'authentification. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Dans ASDM, le volet Interface vous permet de configurer les propriétés de routage OSPF spécifiques à l'interface, telles que l'authentification des messages OSPF et les propriétés. Deux onglets vous aident à configurer les interfaces dans OSPF :

- L'onglet Authentication (Authentification) affiche les renseignements d'authentification OSPF pour les interfaces ASA.
- L'onglet Properties (Propriétés) affiche les propriétés OSPF définies pour chaque interface sous forme de tableau.

Pour configurer les paramètres d'interface OSPFv2, procédez comme suit :

Procédure

Étape 1 Cliquez sur l'onglet **Authentication** (Authentification) pour afficher les renseignements d'authentification OSPF pour les interfaces ASA. Un double clic sur une ligne du tableau ouvre la boîte de dialogue Edit OSPF Authentication Interface (Modifier l'interface d'authentification OSPF) pour l'interface sélectionnée.

Étape 2 Cliquez sur **Edit**.

La boîte de dialogue Edit OSPF Authentication Interface (Modifier l'interface d'authentification OSPF) apparaît. La boîte de dialogue Edit OSPF Interface Authentication (Modifier l'interface d'authentification OSPF) vous permet de configurer le type d'authentification et les paramètres OSPF pour l'interface sélectionnée.

Étape 3 Choisissez le type d'authentification en cliquant sur le bouton radio approprié :

- **No authentication** (Aucune authentification) pour désactiver l'authentification OSPF.
- **Area authentication, if defined** (Authentification de zone, si défini) (par défaut) pour utiliser le type d'authentification spécifié pour la zone. Consultez Configurer les paramètres de zone OSPFv2, à la page 951 pour en savoir plus sur la configuration de l'authentification de zone. L'authentification de zone est désactivée par défaut. Par conséquent, à moins que vous ayez déjà spécifié un type d'authentification de zone, les interfaces définies avec l'authentification de zone ont l'authentification désactivée jusqu'à ce que vous configuriez ce paramètre.
- **Password authentication** (Authentification par mot de passe) pour utiliser l'authentification par mot de passe en texte clair (non conseillé lorsque la sécurité est une préoccupation).
- **MD5 authentication** (Authentification MD5) pour utiliser l'authentification MD5.
- **Key chain authentication** (Authentification par chaîne de clés) pour utiliser l'authentification par chaîne de clés (conseillé). Consultez Configurer une chaîne de clés pour l'authentification, à la page 940 pour en savoir plus sur la configuration de la chaîne de clés pour l'authentification.

Étape 4 Si vous avez choisi l'authentification par mot de passe, dans la zone Authentication Password (Mot de passe d'authentification), saisissez le mot de passe :

a) Dans le champ Enter Password (Saisir le mot de passe), saisissez une chaîne de texte de huit caractères maximum.
b) Dans le champ Re-entrer Password (Saisir à nouveau le mot de passe), resaisissez le mot de passe.

Étape 5 Si vous avez choisi l'authentification de la chaîne de clés, saisissez le nom de la chaîne de clés dans le champ Enter Key chain name (Saisir le nom de la chaîne de clés).

Étape 6 Choisissez les paramètres pour les ID et les clés MD5 dans la zone ID, qui comprend les paramètres pour la saisie des clés et des paramètres MD5 lorsque l'authentification MD5 est activée. Tous les appareils de l'interface qui utilisent l'authentification OSPF doivent utiliser la même clé MD5 et le même ID.

a) Dans le champ Key ID (ID de clé), saisissez un identifiant de clé numérique. Les valeurs valides sont comprises entre 0 et 255. L'ID de clé s'affiche pour l'interface sélectionnée.

b) Dans le champ Key (Clé), saisissez une chaîne de caractères alphanumériques d'une durée maximale de 16 octets. La clé s'affiche pour l'interface sélectionnée.

c) Cliquez sur **Add** (Ajouter) ou **Delete** (Supprimer) pour ajouter ou supprimer la clé MD5 spécifiée au tableau d'ID et de clé MD5.

Étape 7 Cliquez sur **OK.**

Étape 8 Cliquez sur l'onglet **Properties** (Propriétés).

Étape 9 Sélectionnez l'interface que vous souhaitez modifier. Un double clic sur une ligne du tableau ouvre la boîte de dialogue de l'onglet Properties (Propriétés) de l'interface sélectionnée.

Étape 10 Cliquez sur **Edit**.

La boîte de dialogue Edit OSPF Interface Properties (Modifier les propriétés de l'interface OSPF) apparaît. Le champ Interface affiche le nom de l'interface pour laquelle vous configurez les propriétés OSPF. Vous ne pouvez pas modifier ce champ.

Étape 11 Cochez ou décochez la case **Broadcast** (Diffusion) pour préciser que l'interface est une interface de diffusion.

Par défaut, cette case est cochée pour les interfaces Ethernet. Décochez cette case pour désigner l'interface comme une interface point à point de non-diffusion. Définir une interface comme point à point, sans diffusion, vous permet de transmettre des routes OSPF sur des tunnels VPN.

Lorsqu'une interface est configurée comme interface point à point sans diffusion, les restrictions suivantes s'appliquent :

- Vous ne pouvez définir qu'un seul voisin pour l'interface.
- Vous devez configurer manuellement le voisin. Consultez Définir les voisins OSPFv2 statiques, à la page 956 pour de plus amples renseignements.
- Vous devez définir une voie de routage statique pointant vers le point terminal de chiffrement. Consultez Configurer une route statique, à la page 867 pour de plus amples renseignements.
- Si OSPF sur un tunnel est exécuté sur l'interface, OSPF standard avec un routeur en amont ne peut pas être exécuté sur la même interface.
- Vous devez lier la carte de chiffrement à l'interface avant de spécifier le voisin OSPF pour vous assurer que les mises à jour OSPF passent par le tunnel VPN. Si vous liez la carte de chiffrement à l'interface après avoir précisé le voisin OSPF, utilisez la commande **clear local-host all** pour effacer les connexions OSPF afin que les contiguïtés OSPF puissent être établies sur le tunnel VPN.

Étape 12 Configurez les options suivantes :

- Saisissez une valeur dans le champ Cost (Coût) qui détermine le coût d'envoi d'un paquet par l'interface. La valeur par défaut est 10.
- Dans le champ Priority (Priorité), saisissez la valeur de priorité du routeur OSPF.

  Lorsque deux routeurs se connectent à un réseau, tous deux tentent de devenir le routeur désigné. Le périphérique ayant la priorité de routeur la plus élevée devient le routeur désigné. En cas d'égalité, le routeur ayant l'ID de routeur le plus élevé devient le routeur désigné.

  Les valeurs valides pour ce paramètre sont comprises entre 0 et 255. La valeur par défaut est 1. Si vous saisissez 0 pour ce paramètre, le routeur ne pourra pas devenir le routeur désigné ou le routeur de secours désigné. Ce paramètre ne s'applique pas aux interfaces configurées comme interfaces point à point non de diffusion.

En mode de contexte multiple, pour les interfaces partagées, spécifiez 0 pour vous assurer que le périphérique ne devienne pas le routeur désigné. Les instances OSPFv2 ne peuvent pas former de contiguïtés entre elles sur les interfaces partagées.

- Cochez ou décochez la case **MTU Ignore** (Ignorer la MTU).

  OSPF vérifie si les voisins utilisent la même MTU sur une interface commune. Cette vérification est effectuée lorsque les voisins échangent des paquets DBD. Si la MTU de réception dans le paquet DBD est supérieure à la MTU IP configurée sur l'interface entrante, la contiguïté OSPF ne sera pas établie.

- Cochez ou décochez la case **Database Filter** (Filtre de base de données).

  Utilisez ce paramètre pour filtrer l'interface LSA sortante pendant la synchronisation et l'inondation. Par défaut, OSPF inonde les nouveaux LSA sur toutes les interfaces dans la même zone, sauf l'interface sur laquelle le LSA arrive. Dans une topologie entièrement maillée, cette inondation peut gaspiller de la bande passante et entraîner une utilisation excessive de la liaison et de la CPU. Cocher cette case empêche l'inondation OSPF du LSA sur l'interface sélectionnée.

Étape 13 (Facultatif) Cliquez sur **Advanced** (Avancé) pour afficher la boîte de dialogue Edit OSPF Advanced Interface Properties (Modifier les propriétés de l'interface avancée OSPF), qui vous permet de modifier les valeurs de l'intervalle Hello OSPF, de l'intervalle de retransmission, du délai de transmission et de l'intervalle de temps mort.

Généralement, vous n'avez qu'à modifier ces valeurs par défaut si vous rencontrez des problèmes OSPF sur votre réseau.

Étape 14 Dans la section Intervals (Intervalles), saisissez des valeurs pour les éléments suivants :

- L'intervalle Hello, qui spécifie l'intervalle, en secondes, entre les paquets Hello envoyés sur une interface. Plus l'intervalle Hello est petit, plus les changements topologiques sont détectés rapidement, mais plus de trafic est envoyé sur l'interface. Cette valeur doit être la même pour tous les routeurs et serveurs d'accès sur une interface donnée. Les valeurs valides vont de 1 à 8 192 secondes. La valeur par défaut est 10 secondes.
- L'intervalle de retransmission, qui spécifie le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. Lorsqu'un routeur envoie un LSA à son voisin, il le conserve jusqu'à ce qu'il reçoive l'accusé de réception. Si le routeur ne reçoit aucun accusé de réception, il renvoie le LSA. Soyez prudent lors de la définition de cette valeur, sinon une retransmission inutile peut en résulter. La valeur doit être supérieure pour les lignes série et les liaisons virtuelles. Les valeurs valides vont de 1 à 8 192 secondes. La valeur par défaut est de 5 secondes.
- Le délai de transmission, qui spécifie le temps estimé, en secondes, nécessaire pour envoyer un paquet LSA sur l'interface. L'âge des LSA dans le paquet de mise à jour est augmenté de la quantité spécifiée par ce champ avant la transmission. Si le délai n'est pas ajouté avant la transmission sur une liaison, le temps pendant lequel le LSA se propage sur la liaison n'est pas pris en compte. La valeur attribuée doit tenir compte des délais de transmission et de propagation pour l'interface. Ce paramètre a plus d'importance sur les liaisons à très faible vitesse. Les valeurs valides vont de 1 à 8 192 secondes. La valeur par défaut est de 1 seconde.

Étape 15 Dans la section Detecting Lost Neighbors (Détection des voisins perdus), effectuez l'une des opérations suivantes :

- Cliquez sur l'intervalle de configuration dans lequel les paquets Hello ne sont pas reçus avant que le routeur déclare le voisin comme étant en panne. Dans le champ Dead Interval (Intervalle de temps mort), précisez l'intervalle, en secondes, pendant lequel aucun paquet Hello n'est reçu, ce qui amène les voisins

à déclarer un routeur en panne. Les valeurs valides vont de 1 à 8 192 secondes. La valeur par défaut de ce paramètre est quatre fois l'intervalle qui a été défini dans le champ Hello Interval (Intervalle Hello).

- Cliquez sur Send fast hello packets (Envoyer des paquets Hello rapides) dans un intervalle de temps mort de 1 seconde. Dans le champ Hello multiplier (Multiplicateur Hello), spécifiez le nombre de paquets Hello à envoyer par seconde. Les valeurs valides sont comprises entre 3 et 20.

Configurer les paramètres de zone OSPFv2

Vous pouvez configurer plusieurs paramètres de zone OSPF. Ces paramètres de zone (indiqués dans la liste des tâches suivante) comprennent la définition de l'authentification, la définition des zones tampons et l'affectation de coûts spécifiques à la route récapitulative par défaut. L'authentification offre une protection par mot de passe contre l'accès non autorisé à une zone.

Les zones tampons sont des zones dans lesquelles les informations sur les routages externes ne sont pas envoyées. Au lieu de cela, une route externe par défaut est générée par l'ABR dans la zone tampon pour les destinations externes au système autonome. Pour tirer parti de la prise en charge de la zone tampon OSPF, le routage par défaut doit être utilisé dans la zone tampon.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Area/Networks** (Zone/Réseaux).

La boîte de dialogue Add OSPF Area (Ajouter une zone OSPF) apparaît.

Étape 3 Choisissez l'une des options suivantes pour le type de zone :

- **Normal** pour faire de la zone une zone OSPF standard. Cette option est sélectionnée par défaut lorsque vous créez une zone pour la première fois.
- **Stub** (Tampon) pour faire de la zone une zone tampon. Les zones tampons ne comportent aucun routeur ni aucune zone au-delà. Les zones tampons empêchent les LSA externes de l'AS (LSA de type 5) d'être submergées dans la zone tampon. Lorsque vous créez une zone tampon, vous avez la possibilité d'empêcher l'inondation des LSA (types 3 et 4) récapitulatifs dans la zone en décochant la case Summary (Résumé).
- **Summary** (Résumé) Pour empêcher l'envoi de LSA dans la zone tampon lorsque la zone définie est une zone tampon, décochez cette case. Par défaut, cette case est cochée pour les zones tampons.
- **NSSA** pour faire de la zone une zone moins dense. Les contrats NSSA acceptent les LSA de type 7. Lorsque vous créez le NSSA, vous avez la possibilité d'empêcher l'inondation des LSA récapitulatifs dans la zone en décochant la case Summary (Résumé). Vous pouvez également désactiver la redistribution de routes en décochant la case Redistribute (Redistribuer) mais en cochant la case Default Information Originate (Origine des informations par défaut).

Étape 4 Saisissez l'adresse IP dans le champ IP Address (Adresse IP) du réseau ou de l'hôte à ajouter à la zone. Utilisez **0.0.0.0** avec un masque réseau de **0.0.0.0** pour créer la zone par défaut. Vous ne pouvez saisir **0.0.0.0** que dans une zone.

Étape 5 Saisissez le masque réseau dans le champ Network Mask (Masque réseau) de l'adresse IP ou de l'hôte à ajouter à la zone. Si vous ajoutez un hôte, choisissez le masque **255.255.255.255**.

Étape 6 Choisissez le type d'authentification OSPF parmi les options suivantes :

- **None** (Aucun) pour désactiver l'authentification de zone OSPF. Il s'agit du paramètre par défaut.
- **Password** (Mot de passe) pour fournir un mot de passe en clair pour l'authentification de zone, ce qui n'est pas conseillé lorsque la sécurité est un problème.
- **MD5** pour permettre l'authentification MD5.

Étape 7 Saisissez une valeur dans le champ Default Cost (Coût par défaut) pour spécifier un coût par défaut pour la zone OSPF.

Cette valeur peut être comprise entre 0 et 65 535. La valeur par défaut est 1.

Étape 8 Cliquez sur **OK**.

Configurer les règles de filtre OSPFv2

Utilisez la procédure suivante pour filtrer les routes ou les réseaux reçus ou transmis dans les mises à jour OSPF.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Filter Rules (Règles de filtre)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Sélectionnez l'ID de processus OSPF dans **OSPF AS** (AS OSPF).

Étape 4 Choisissez une liste d'accès standard dans la lise déroulante Access List (Liste d'accès). Cliquez sur **Manage** (Gérer) pour ajouter une nouvelle ACL.

Étape 5 Choisissez une direction dans la liste déroulante Direction. La direction spécifie si le filtre doit être appliqué aux mises à jour entrantes ou sortantes.

Étape 6 Pour les filtres entrants, vous pouvez éventuellement spécifier une interface pour limiter le filtre aux mises à jour reçues sur cette interface.

Étape 7 Pour les filtres sortants, vous pouvez éventuellement spécifier les types de routes distribués.

a) Choisissez une option dans la liste déroulante Protocol (Protocole).

Vous pouvez choisir un protocole de routage, par exemple, **BGP**, **EIGRP**, **OSPF** ou **RIP**.

Choisissez **Connected** (Connecté) pour filtrer les homologues et les réseaux appris par le biais des routes connectées.

Choisissez **Static** (Statique) pour filtrer les homologues et les réseaux appris par le biais des routes statiques.

b) Si vous avez choisi BGP, EIGRP ou OSPF, choisissez également le **Process ID** (ID de processus) pour ce protocole.

Étape 8 Cliquez sur **OK**.

Étape 9 Cliquez sur **Apply** (Appliquer).

Configurer une NSSA OSPFv2

La mise en œuvre du protocole OSPFv2 d'une zone NSSA est similaire à une zone tampon OSPFv2. NSSA n'inonde pas les LSA externes de type 5 du cœur vers la zone, mais il peut importer des routes externes du système autonome de manière limitée dans la zone.

NSSA importe des routes externes du système autonome de type 7 dans une zone NSSA par redistribution. Ces LSA de type 7 sont traduites en LSA de type 5 par les ABR de NSSA, qui sont inondés dans tout le domaine de routage. La synthèse et le filtrage sont pris en charge pendant la traduction.

Vous pouvez simplifier l'administration si vous êtes un FAI ou un administrateur réseau qui doit connecter un site central à l'aide du protocole OSPFv2 à un site distant qui utilise un protocole de routage différent avec NSSA.

Avant la mise en œuvre de NSSA, la connexion entre le routeur de frontière du site d'entreprise et le routeur distant ne pouvait pas être exécutée en tant que zone tampon OSPFv2, car les routes du site distant ne pourraient pas être redistribuées dans la zone tampon, et deux protocoles de routage devaient être maintenus. Un protocole simple comme RIP était généralement exécuté et gérait la redistribution. Avec NSSA, vous pouvez étendre le protocole OSPFv2 pour couvrir la connexion à distance en définissant la zone entre le routeur d'entreprise et le routeur distant en tant que NSSA.

Veuillez consulter les lignes directrices suivantes avant d'utiliser cette fonctionnalité :

- Vous pouvez définir une route par défaut de type 7 qui peut être utilisée pour atteindre des destinations externes. Une fois configuré, le routeur génère une valeur par défaut de type 7 dans le NSSA ou le routeur de limite de zone NSSA.
- Tous les routeurs d'une même zone doivent convenir que la zone est NSSA; sinon, les routeurs ne peuvent pas communiquer entre eux.

Procédure

Étape 1 Depuis la page d'accueil principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Area/Networks** (Zone/Réseaux).

Étape 3 Cliquez sur **Add** (ajouter).

La boîte de dialogue Add OSPF Area (Ajouter une zone OSPF) apparaît.

Étape 4 Cliquez sur le bouton radio **NSSA** dans la zone Area Type (Type de zone).

Choisissez cette option pour faire de la zone une zone NSSA (not-so-stubby area). Les contrats NSSA acceptent les LSA de type 7. Lorsque vous créez le NSSA, vous avez la possibilité d'empêcher l'inondation des LSA récapitulatifs dans la zone en décochant la case Summary (Résumé). Vous pouvez également désactiver la redistribution de routes en décochant la case Redistribute (Redistribuer) mais en cochant la case Default Information Originate (Origine des informations par défaut).

Étape 5 Saisissez l'adresse IP dans le champ IP Address (Adresse IP) du réseau ou de l'hôte à ajouter à la zone. Utilisez **0.0.0.0** avec un masque réseau de **0.0.0.0** pour créer la zone par défaut. Vous ne pouvez saisir **0.0.0.0** que dans une zone.

Étape 6 Saisissez le masque réseau dans le champ Network Mask (Masque réseau) de l'adresse IP ou de l'hôte à ajouter à la zone. Si vous ajoutez un hôte, choisissez le masque **255.255.255.255**.

Étape 7 Dans la zone Authentication (Authentification), cliquez sur le bouton radio **None** (Aucun) pour désactiver l'authentification de zone OSPF.

Étape 8 Saisissez une valeur dans le champ Default Cost (Coût par défaut) pour spécifier un coût par défaut pour la zone OSPF.

Cette valeur peut être comprise entre 0 et 65 535. La valeur par défaut est 1.

Étape 9 Cliquez sur **OK**.

Configurer un ensemble d'adresses IP pour la mise en grappe (OSPFv2 et OSPFv3)

Vous pouvez attribuer une plage d'adresses IPv4 pour le regroupement de grappes d'ID de routeur si vous utilisez la mise en grappe d'interfaces individuelles.

Pour attribuer une plage d'adresses IPv4 à l'ensemble de grappes d'ID de routeur dans l'interface individuelle pour le protocole OSPFv2, procédez comme suit :

Procédure

Étape 1 Depuis la page d'accueil principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF) apparaît.

Étape 4 Cliquez sur le bouton radio **Cluster Pool** (Ensemble de grappes). Si vous utilisez la mise en grappe, vous n'avez pas besoin de spécifier d'ensemble d'adresses IP pour l'ID de routeur (c'est-à-dire, laissez le champ vide). Si vous ne saisissez pas d'ensemble d'adresses IP, l'ASA utilise l'ID de routeur généré automatiquement.

Étape 5 Saisissez le nom de l'ensemble d'adresses IP ou cliquez sur les points de suspension pour afficher la boîte de dialogue Select IP Address Pool (Sélectionner un ensemble d'adresses IP).

Étape 6 Cliquez deux fois sur un nom d'ensemble d'adresses IP existant pour l'ajouter au champ Assign (Affecter). Sinon, cliquez sur **Add** (Ajouter) pour créer un nouvel ensemble d'adresses IP.

La boîte de dialogue Add IPv4 Pool (Ajouter un ensemble IPv4) s'affiche.

Étape 7 Saisissez le nom du nouvel ensemble d'adresses IP dans le champ **Name** (Nom).

Étape 8 Saisissez l'adresse IP de départ ou cliquez sur les points de suspension pour afficher la boîte de dialogue Browse Starting IP Address (Parcourir l'adresse IP de départ).

Étape 9 Cliquez deux fois sur une entrée pour l'ajouter dans le champ Starting IP Address (Adresse IP de départ), puis cliquez sur **OK**.

Étape 10 Saisissez l'adresse IP de fin ou cliquez sur les points de suspension pour afficher la boîte de dialogue Browse Ending IP Address (Parcourir l'adresse IP de fin).

Étape 11 Cliquez deux fois sur une entrée pour l'ajouter au champ Ending IP Address (Adresse IP de fin), puis cliquez sur **OK**.

Étape 12 Dans la liste déroulante, choisissez le filtre d'adresse locale, puis cliquez sur **OK**.

Le nouvel ensemble d'adresses IP apparaît dans la liste Select IP Address Pool (Sélectionner un ensemble d'adresses IP).

Étape 13 Cliquez deux fois sur le nom du nouvel ensemble d'adresses IP pour l'ajouter au champ Assign (Affecter), puis cliquez sur **OK**.

Le nom du nouvel ensemble d'adresses IP apparaît dans le champ Cluster Pool (Ensemble de grappes) de la boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF).

Étape 14 Cliquez sur **OK**.

Étape 15 Si vous souhaitez modifier les paramètres de l'ensemble d'adresses IP nouvellement ajouté, cliquez sur **Edit** (Modifier).

La boîte de dialogue Edit IPv4 Pool (Modifier un ensemble IPv4) s'affiche.

Étape 16 Répétez les étapes 4 à 14.

Remarque Vous ne pouvez pas modifier ni supprimer un ensemble d'adresses IP existant qui a été attribué et qui est déjà utilisé par un ou plusieurs profils de connexion.

Étape 17 Cliquez sur **OK**.

Étape 18 Pour attribuer une plage d'adresses IPv4 à l'ensemble de grappes d'ID de routeur dans la mise en grappe d'interfaces individuelles pour le protocole OSPFv3, procédez comme suit :

a) Depuis la page d'accueil principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

b) Cliquez sur l'onglet **Process Instances** (Instances de processus).

c) Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

d) Sélectionnez l'option Cluster Pool (Ensemble de grappes) dans la liste déroulante Router ID (ID de routeur). Si vous n'avez pas besoin de spécifier d'ensemble d'adresses IP pour l'ID de routeur, sélectionnez l'option Automatic (Automatique). Si vous ne configurez pas d'ensemble d'adresses IP, l'ASA utilise l'ID de routeur généré automatiquement.

e) Saisissez le nom de l'ensemble d'adresses IP. Sinon, cliquez sur les points de suspension pour afficher la boîte de dialogue Select IP Address Pool (Sélectionner un ensemble d'adresses IP).

f) Cliquez deux fois sur un nom d'ensemble d'adresses IP existant pour l'ajouter au champ Assign (Affecter). Sinon, cliquez sur **Add** (Ajouter) pour créer un nouvel ensemble d'adresses IP.

La boîte de dialogue Add IPv4 Pool (Ajouter un ensemble IPv4) s'affiche.

g) Saisissez le nom du nouvel ensemble d'adresses IP dans le champ **Name** (Nom).
h) Saisissez l'adresse IP de départ ou cliquez sur les points de suspension pour afficher la boîte de dialogue Browse Starting IP Address (Parcourir l'adresse IP de départ).
i) Cliquez deux fois sur une entrée pour l'ajouter dans le champ Starting IP Address (Adresse IP de départ), puis cliquez sur **OK**.
j) Saisissez l'adresse IP de fin ou cliquez sur les points de suspension pour afficher la boîte de dialogue Browse Ending IP Address (Parcourir l'adresse IP de fin).
k) Cliquez deux fois sur une entrée pour l'ajouter au champ Ending IP Address (Adresse IP de fin), puis cliquez sur **OK**.
l) Dans la liste déroulante, choisissez le filtre d'adresse locale, puis cliquez sur **OK**.

   Le nouvel ensemble d'adresses IP apparaît dans la liste Select IP Address Pool (Sélectionner un ensemble d'adresses IP).

m) Cliquez deux fois sur le nom du nouvel ensemble d'adresses IP pour l'ajouter au champ Assign (Affecter), puis cliquez sur **OK**.

   Le nom du nouvel ensemble d'adresses IP apparaît dans le champ Cluster Pool (Ensemble de grappes) de la boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF).

n) Cliquez sur **OK**.
o) Si vous souhaitez modifier les paramètres de l'ensemble de grappes nouvellement ajouté, cliquez sur **Edit** (Modifier).

   La boîte de dialogue Edit IPv4 Pool (Modifier un ensemble IPv4) s'affiche.

p) Répétez les étapes 4 à 14.

Remarque Vous ne pouvez pas modifier ou supprimer un ensemble d'adresses IP existant qui a été attribué et qui est déjà utilisé par un autre processus OSPFv3.

q) Cliquez sur **OK**.

Définir les voisins OSPFv2 statiques

Vous devez définir des voisins OSPFv2 statiques pour annoncer les routes OSPFv2 sur un réseau point à point de non-diffusion. Cette fonctionnalité vous permet de diffuser des annonces OSPFv2 sur une connexion VPN existante sans avoir à encapsuler les annonces dans un tunnel GRE.

Avant de commencer, vous devez créer une route statique vers le voisin OSPFv2. Consultez Configurer une route statique, à la page 867 pour en savoir plus sur la création des routes statiques.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Static Neighbor (Voisin statique)**.

Étape 2 Cliquez sur **Add** ou **Edit** (ajouter ou modifier).

La boîte de dialogue Add/Edit OSPF Neighbor Entry (Ajouter/modifier une entrée de voisin OSPF) s'affiche. Cette boîte de dialogue vous permet de définir un nouveau voisin statique ou de modifier les renseignements d'un voisin statique existant. Vous devez définir un voisin statique pour chaque interface point à point de non-diffusion. Notez les restrictions suivantes :

- Vous ne pouvez pas définir le même voisin statique pour deux processus OSPF différents.
- Vous devez définir une route statique pour chaque voisin statique.

Étape 3 Dans la liste déroulante OSPF Process (Processus OSPF), choisissez le processus OSPF associé au voisin statique. Si vous modifiez un voisin statique existant, vous ne pouvez pas modifier cette valeur.

Étape 4 Dans le champ **Neighbor** (Voisin), saisissez l'adresse IP du voisin statique.

Étape 5 Dans le champ **Interface**, choisissez l'interface associée au voisin statique. Si vous modifiez un voisin statique existant, vous ne pouvez pas modifier cette valeur.

Étape 6 Cliquez sur **OK**.

Configurer les minuteries de calcul de routage

Vous pouvez configurer le délai entre le moment où le protocole OSPFv2 reçoit une modification de topologie et le moment où il démarre un calcul SPF. Vous pouvez également configurer le délai de rétention entre deux calculs SPF consécutifs.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF) apparaît.

Étape 4 La zone Timers (Minuteries) vous permet de modifier les paramètres utilisés pour configurer les minuteries de calcul de cadence et de SPF. Dans la zone Timers (Minuteries), saisissez les valeurs suivantes :

- Le délai SPF initial spécifie le temps (en millisecondes) entre le moment où OSPF reçoit une modification de topologie et le moment où le calcul SPF commence. Les valeurs valides vont de 0 à 600 000 millisecondes.
- Le délai de rétention SPF minimum spécifie le délai de rétention (en millisecondes) entre des calculs SPF consécutifs. Les valeurs valides sont comprises entre 0 et 600 000 millisecondes.
- Le délai d'attente SPF maximum spécifie le temps d'attente maximum entre deux calculs SPF consécutifs. Les valeurs valides vont de 0 à 600 000 millisecondes.

Étape 5 Cliquez sur **OK**.

Journaliser les voisins en hausse ou en baisse

Par défaut, un message de journal système est généré lorsqu'un voisin OSPFv2 redevient disponible ou tombe en panne.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF) apparaît.

Étape 4 La zone Adjacency Changes (Modifications de contiguïté) comprend des paramètres qui définissent les modifications de contiguïté provoquant l'envoi des messages de journal système. Dans la zone Adjacency Changes (Modifications de contiguïté), saisissez les valeurs suivantes :

- Cochez la case **Log Adjacency Changes** (Journaliser les modifications de contiguïté) pour que l'ASA envoie un message de journal système à chaque fois qu'un voisin OSPFv2 est activé ou désactivé. Ce paramètre est coché par défaut.
- Cochez la case **Log Adjacency Changes Detail** (Journaliser les détails sur le changement de contiguïté) pour que l'ASA envoie un message de journal système chaque fois qu'un changement d'état se produit, pas seulement quand un voisin est activé ou désactivé. Ce paramètre est décoché par défaut.

Étape 5 Cliquez sur **OK**.



Remarque La journalisation doit être activée pour que les messages de voisin activé ou désactivé soient envoyés.

Configurer une chaîne de clés pour l'authentification

Pour améliorer la sécurité et la protection des données des périphériques, vous pouvez activer des clés changeantes pour l'authentification des homologues IGP. Les clés pivotantes empêchent tout utilisateur malveillant de deviner les clés utilisées pour l'authentification du protocole de routage, protégeant ainsi le réseau contre les annonces de routage incorrect et la redirection du trafic. La modification fréquente des clés réduit le risque qu'elles finissent par être devinées. Lors de la configuration de l'authentification pour les protocoles de routage qui fournissent des chaînes de clés, configurez les clés d'une chaîne de clés pour qu'elles se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active.

Si la durée de vie de la clé expire et qu'aucune clé active n'est trouvée, OSPF utilise la dernière clé valide pour maintenir la contiguïté avec les homologues.

Cette section décrit comment créer une chaîne de clés pour l'authentification des homologues OSPF. Cette section couvre également les étapes pour ajouter ou modifier les attributs d'une chaîne de clés. Après avoir configuré un objet de chaîne de clés, vous pouvez l'utiliser pour définir l'authentification OSPFv2 pour une interface et pour une liaison virtuelle. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie. Pour savoir comment définir l'authentification pour une interface, consultez Configurer les paramètres d'interface OSPFv2, à la page 947; pour une liaison virtuelle, consultez Configurer un lien virtuel dans OSPF, à la page 961.

Pour configurer une chaîne de clés, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Key Chain (Chaîne de clés)** .

Étape 2 Dans la section **Configure Key Chain** (Configurer la chaîne de clés), cliquez sur **Add** (Ajouter).

Étape 3 Saisissez le nom de la chaîne de clés dans la boîte de dialogue **Add Key Chain** (Ajouter une chaîne de clés), puis cliquez sur **OK**.

Le nom de la chaîne de clés créée est répertorié dans la grille **Configure Key Chain** (Configurer la chaîne de clés).

Étape 4 Sélectionnez le nom de la chaîne de clés dans la section **Configure Key Chain** (Configurer la chaîne de clés), et dans la section **Configure Key** (Configurer la clé), cliquez sur **Add** (Ajouter). Pour modifier une clé existante, sélectionnez le nom de la clé et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Add Key** (Ajouter une clé) ou **Edit Key** (Modifier une clé) apparaît, selon l'action que vous avez sélectionnée.

Étape 5 Précisez l'identifiant de clé dans le champ **Key ID**.

La valeur de l'ID de clé peut être comprise entre 0 et 255. Utilisez la valeur 0 uniquement lorsque vous souhaitez signaler une clé non valide.

Remarque Vous ne pouvez pas modifier un ID de clé enregistré.

Étape 6 Dans la liste déroulante **Cryptographic Algorithm** (Algorithme cryptographique), choisissez **MD5**. MD5 est le seul algorithme pris en charge pour l'authentification de la chaîne de clés.

Étape 7 Sélectionnez le type de chiffrement en cliquant sur le bouton radio **Plain Text** (Texte brut) ou **Encrypted** (Chiffré), puis saisissez le mot de passe dans le champ **Authentication Key** (Clé d'authentification).

- Même si la chaîne de clé peut contenir 80 caractères, seul un maximum de 64 caractères est autorisé pour l'authentification OSPF.
- Les mots de passe ne peuvent pas être un seul chiffre ni ceux commençant par un chiffre suivi d'un espace. Par exemple, « 0 pass » ou « 1 » ne sont pas valides.

Étape 8 Fournissez les valeurs de durée de vie dans les champs **Accept Lifetime** (Accepter la durée de vie) et **Send Lifetime** (Envoyer la durée de vie) :

Vous pouvez spécifier l'intervalle de temps nécessaire pour que le périphérique accepte ou envoie la clé lors de l'échange de clés avec un autre périphérique. L'heure de fin peut correspondre à la durée absolue à laquelle la durée de vie de l'acceptation/envoi se termine ou n'expire jamais.

Voici les règles de validation pour les valeurs de début et de fin :

- La durée de vie de début ne peut pas être nulle lorsque la fin de vie est spécifiée.
- La durée de vie de début pour l'acceptation ou l'envoi de la durée de vie doit être antérieure à la fin de vie.

Étape 9 Pour enregistrer les attributs de la chaîne de clés, cliquez sur **OK**. Dans la page **Key Chain** (Chaîne de clés), cliquez sur **Appy** (Appliquer).

Prochaine étape

Vous pouvez maintenant appliquer la chaîne de clés configurée pour définir l'authentification OSPFv2 pour une interface et pour la liaison virtuelle.

- Configurer les paramètres d'interface OSPFv2, à la page 947
- Configurer un lien virtuel dans OSPF, à la page 961

Configurer le filtrage dans OSPF

Le volet Filtering (Filtrage) affiche les filtres LSA ABR de type 3 qui ont été configurés pour chaque processus OSPF.

Les filtres LSA ABR de type 3 permettent uniquement l'envoi de préfixes spécifiés d'une zone à une autre et restreignent tous les autres préfixes. Ce type de filtrage de zone peut être appliqué hors d'une zone OSPF spécifique, dans une zone OSPF spécifique ou à la fois vers et depuis les mêmes zones OSPF.

Le filtrage LSA OSPF ABR de type 3 améliore votre contrôle de la distribution des routages entre les zones OSPF.

Remarque Seuls les LSA de type 3 qui proviennent d'un ABR sont filtrés.

Pour configurer le filtrage dans OSPF, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Filtering (Filtrage)**.

Étape 2 Cliquez sur **Add** ou **Edit**(ajouter ou modifier) .

La boîte de dialogue Add or Edit OSPF Filtering Entry (Ajouter ou modifier une entrée de filtrage OSPF) vous permet d'ajouter de nouveaux filtres au tableau de filtres ou de modifier un filtre existant. Certains renseignements de filtrage ne peuvent pas être modifiés lorsque vous modifiez un filtre existant.

Étape 3 Choisissez le processus OSPF associé à l'entrée de filtre dans la liste déroulante OSPF Process (Processus OSPF).

Étape 4 Choisissez l'ID de zone associé à l'entrée de filtre dans la liste déroulante Area ID (ID de zone). Si vous modifiez une entrée de filtre existante, vous ne pouvez pas modifier ce paramètre.

Étape 5 Choisissez une liste de préfixes dans la liste déroulante Prefix List (Liste des préfixes).

Étape 6 Choisissez la direction du trafic filtrée dans la liste déroulante Traffic Direction (Direction du trafic).

Choisissez entrant pour filtrer les LSA entrant dans une zone OSPF, ou sortant pour filtrer les LSA sortant d'une zone OSPF. Si vous modifiez une entrée de filtre existante, vous ne pouvez pas modifier ce paramètre.

Étape 7 Cliquez sur **Manage** (Gérer) pour afficher la boîte de dialogue Configure Prefix Lists (Configurer les listes de préfixes), dans laquelle vous pouvez ajouter, modifier ou supprimer des listes de préfixes et des règles de préfixes. Pour plus de renseignements, consultez Configurer les listes de préfixe, à la page 890 et Configurer les valeurs de mesure pour une action de routage, à la page 891.

Étape 8 Cliquez sur **OK**.

Configurer un lien virtuel dans OSPF

Si vous ajoutez une zone à un réseau OSPF et qu'il n'est pas possible de connecter la zone directement à la zone du réseau fédérateur, vous devez créer une liaison virtuelle. Une liaison virtuelle connecte deux appareils OSPF qui ont une zone commune, appelée la zone de transit. Un des appareils OSPF doit être connecté à la zone du réseau fédérateur.

Pour définir de nouvelles liaisons virtuelles ou modifier les propriétés des liaisons virtuelles existantes, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Virtual Link (Liaison virtuelle)**.

Étape 2 Cliquez sur **Add** ou **Edit** (ajouter ou modifier).

La boîte de dialogue Add or Edit OSPF Virtual Link (Ajouter ou modifier une liaison virtuelle OSPF) apparaît. Elle vous permet de définir de nouvelles liaisons virtuelles ou de modifier les propriétés des liaisons virtuelles existantes.

Étape 3 Choisissez l'ID de processus OSPF associé à la liaison virtuelle dans la liste déroulante OSPF Process (Processus OSPF). Si vous modifiez une liaison virtuelle existante, vous ne pouvez pas modifier ce paramètre.

Étape 4 Choisissez l'ID de zone associé à la liaison virtuelle dans la liste déroulante Area ID (ID de zone).

Choisissez la zone partagée par les appareils OSPF voisins. La zone sélectionnée ne peut pas être une zone NSSA ou une zone de stub. Si vous modifiez une liaison virtuelle existante, vous ne pouvez pas modifier ce paramètre.

Étape 5 Dans le champ **Peer Router ID** (ID de routeur homologue), saisissez l'ID de routeur du voisin de liaison virtuelle.

Si vous modifiez une liaison virtuelle existante, vous ne pouvez pas modifier ce paramètre.

Étape 6 Cliquez sur **Advanced** (Avancé) pour modifier les propriétés de liaison virtuelle avancées.

La boîte de dialogue Advanced OSPF Virtual Link Properties (Propriétés de liaison virtuelle OSPF avancées) apparaît. Vous pouvez configurer les propriétés OSPF pour la liaison virtuelle dans cette zone. Ces propriétés comprennent les paramètres d'authentification et d'intervalle de paquets.

Étape 7 Dans la zone Authentication (Authentification), choisissez le type d'authentification en cliquant sur le bouton radio à côté de l'une des options suivantes :

- **No authentication** (Aucune authentification) pour désactiver l'authentification OSPF.
- **Password authentication** (Authentification par mot de passe) pour utiliser l'authentification par mot de passe en texte clair (non conseillé lorsque la sécurité est une préoccupation).
- **MD5 authentication** (Authentification MD5) pour utiliser l'authentification MD5.
- **Key chain authentication** (Authentification par chaîne de clés) pour utiliser l'authentification par chaîne de clés (conseillé). Consultez Configurer une chaîne de clés pour l'authentification, à la page 940 pour en savoir plus sur la configuration de la chaîne de clés pour l'authentification.

Étape 8 Dans la zone Authentication Password (Mot de passe d'authentification), entrez et reconfirmez un mot de passe lorsque l'authentification par mot de passe est activée. Les mots de passe doivent être des chaînes de texte de 8 caractères maximum.

Étape 9 Dans la zone MD5 IDs and Key (ID et clé MD5), saisissez les clés et les paramètres MD5 lorsque l'authentification MD5 est activée. Tous les appareils de l'interface qui utilisent l'authentification OSPF doivent utiliser la même clé MD5 et le même ID. Spécifiez les paramètres suivants :

a) Dans le champ **Key ID** (ID de clé), saisissez un identifiant de clé numérique. Les valeurs valides sont comprises entre 0 et 255. L'ID de clé s'affiche pour l'interface sélectionnée.
b) Dans le champ **Key** (Clé), saisissez une chaîne de caractères alphanumériques d'une durée maximale de 16 octets. L'ID de clé s'affiche pour l'interface sélectionnée.
c) Cliquez sur **Add** (Ajouter) ou **Delete** (Supprimer) pour ajouter ou supprimer la clé MD5 spécifiée au tableau d'ID et de clé MD5.

Étape 10 Dans la zone Interval (Intervalle), spécifiez la synchronisation de l'intervalle pour le paquet en choisissant parmi les options suivantes :

- **Hello Interval** (Intervalle Hello) pour spécifier l'intervalle, en secondes, entre les paquets Hello envoyés sur une interface. Plus l'intervalle Hello est petit, plus les changements topologiques sont détectés rapidement, mais plus le trafic acheminé sur l'interface est important. Cette valeur doit être la même pour tous les routeurs et serveurs d'accès sur une interface donnée. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est 10 secondes.
- **Retransmit Interval** (Intervalle de retransmission) pour spécifier le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. Lorsqu'un routeur envoie un LSA à son voisin, il le conserve jusqu'à ce qu'il reçoive l'accusé de réception. Si le routeur ne reçoit aucun accusé de réception, il renvoie le LSA. Soyez prudent lors de la définition de cette valeur, sinon une retransmission inutile peut en résulter. La valeur doit être supérieure pour les lignes série et les liaisons virtuelles. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.

- **Transmit Delay** (Délai de transmission) pour spécifier le temps estimé, en secondes, nécessaire pour envoyer un paquet LSA sur l'interface. L'âge des LSA dans le paquet de mise à jour est augmenté de la quantité spécifiée par ce champ avant la transmission. Si le délai n'est pas ajouté avant la transmission sur une liaison, le temps pendant lequel le LSA se propage sur la liaison n'est pas pris en compte. La valeur attribuée doit tenir compte des délais de transmission et de propagation pour l'interface. Ce paramètre a plus d'importance sur les liaisons à très faible vitesse. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 1 seconde.
- **Dead Interval** (Intervalle de temps mort) pour spécifier l'intervalle, en secondes, pendant lequel aucun paquet Hello n'est reçu, ce qui amène les voisins à déclarer un routeur en panne. Cette valeur peut être comprise entre 1 et 65 535. La valeur par défaut de ce champ est quatre fois l'intervalle défini par le champ Hello Interval (Intervalle Hello).

Étape 11 Cliquez sur **OK**.

Configurer le protocole OSPFv3

Cette section décrit les tâches nécessaires à la configuration d'un processus de routage OSPFv3.

Activer OSPFv3

Pour activer OSPFv3, vous devez créer un processus de routage OSPFv3, créer une zone pour OSPFv3, activer une interface pour OSPFv3, puis redistribuer la route dans les processus de routage OSPFv3 ciblés.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Sous l'onglet Process Instances (Instances de processus), cochez la case **Enable OSPFv3 Process** (Activer le processus OSPFv3). Vous pouvez activer jusqu'à deux instances de processus OSPF. Seul le mode de contexte unique est pris en charge.

Étape 3 Saisissez un ID de processus dans le champ Process ID (ID de processus). L'ID peut être n'importe quel entier positif.

Étape 4 Cliquez sur **Apply** pour enregistrer vos modifications.

Étape 5 Pour continuer, consultez Configurer les paramètres de zone OSPFv3, à la page 965.

Configurer les paramètres d'interface OSPFv3

Vous pouvez modifier certains paramètres OSPFv3 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : l'intervalle Hello et l'intervalle Dead. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Interfaces**.

Étape 2 Cliquez sur l'onglet **Authentication** (Authentification).

Étape 3 Pour spécifier les paramètres d'authentification pour une interface, sélectionnez l'interface et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit OSPFv3 Interface Authentication** (modifier l'authentification de l'interface OSPFv3) apparaît.

Étape 4 Choisissez le type d'authentification à partir de la liste déroulante **Authentication Type** (Type d'authentification). Les options disponibles sont Zone, Interface et Aucun. L'option Aucun indique qu'aucune authentification n'est utilisée.

Étape 5 Choisissez l'algorithme d'authentification dans la liste déroulante **Authentication Algorithm** (Algorithme d'authentification). Les valeurs prises en charge sont SHA-1 et MD5.

Étape 6 Saisissez la clé d'authentification dans le champ **Authentication Key** (Clé d'authentification). Lorsque l'authentification MD5 est utilisée, la clé doit comporter 32 chiffres hexadécimaux (16 octets). Lorsque l'authentification SHA-1 est utilisée, la clé doit comporter 40 chiffres hexadécimaux (20 octets).

Étape 7 Choisissez l'algorithme de chiffrement dans la liste déroulante **Encryption Algorithm** (Algorithme de chiffrement). Les valeurs prises en charge sont AES-CD, 3DES et DES. L'entrée NULL indique qu'il n'y a pas de chiffrement.

Étape 8 Saisissez la clé de chiffrement dans le champ **Encryption Key** (Clé de chiffrement).

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur l'onglet **Properties** (Propriétés).

Étape 11 Sélectionnez l'interface dont vous souhaitez modifier les propriétés, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Edit OSPFv3 Interface Properties (Modifier les propriétés de l'interface OSPFv3) apparaît.

Étape 12 Cochez la case **Enable OSPFv3 on this interface** (Activer le protocole OSPFv3 sur cette interface).

Étape 13 Choisissez l'ID de processus à partir de la liste déroulante.

Étape 14 Choisissez l'ID de zone à partir de la liste déroulante.

Étape 15 (Facultatif) Spécifiez l'ID d'instance de zone à affecter à l'interface. Une interface ne peut avoir qu'une seule zone OSPFv3. Vous pouvez utiliser la même zone sur plusieurs interfaces, et chaque interface peut utiliser un ID d'instance de zone différent.

Étape 16 Choisissez le type de réseau dans la liste déroulante. Les options prises en charge sont par défaut, diffusion et point à point.

Étape 17 Saisissez le coût d'envoi d'un paquet sur une interface dans le champ Cost (Coût).

Étape 18 Saisissez la priorité du routeur, qui aide à déterminer le routeur désigné pour un réseau dans le champ Priority (Priorité). Les valeurs valides sont comprises entre 0 et 255.

Étape 19 Cochez la case **Disable MTU mismatch detection** (Désactiver la détection de la non-concordance MTU) pour désactiver la détection de la non-concordance MTU OSPF lors de la réception de paquets DBD. La détection des incompatibilités MTU OSPF est activée par défaut.

Étape 20 Cochez la case **Filter outgoing link state advertisements** (Filtrer les annonces d'état de liaison sortantes) pour filtrer les LSA sortants vers une interface OSPFv3. Tous les LSA sortants sont acheminés vers l'interface par défaut.

Étape 21 Cochez la case **OSPF Flood Reduction** (Réduction des inondations OSPF) pour réduire les inondations de données inutiles et l'actualisation des LSA de l'interface.

Étape 22 Dans la zone **Timers** (Minuteries), dans le champ **Dead Interval** (Intervalle de temps mort), saisissez la période en secondes pendant laquelle les paquets Hello ne doivent pas être vus avant que les voisins indiquent que le routeur est en panne. La valeur doit être la même pour tous les nœuds du réseau et peut varier de 1 à 65 535.

Étape 23 Dans le champ **Hello Interval** (Intervalle Hello), saisissez l'intervalle en secondes entre les paquets Hello envoyés sur l'interface. La valeur doit être la même pour tous les nœuds d'un réseau spécifique et peut varier de 1 à 65535. L'intervalle par défaut est de 10 secondes pour les interfaces Ethernet et de 30 secondes pour les interfaces de non-diffusion.

Étape 24 Dans le champ **Retransmit Interval** (Intervalle de retransmission), saisissez le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. La durée doit être supérieure au délai aller-retour attendu entre deux routeurs du réseau connecté. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.

Étape 25 Dans le champ **Transmit Delay** (Délai de transmission), saisissez la durée estimée en secondes pour envoyer un paquet de mise à jour d'état de liaison sur l'interface. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 1 seconde.

Étape 26 Cliquez sur **OK**.

Étape 27 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer les paramètres de zone OSPFv3

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Areas** (Zones).

Étape 3 Pour ajouter une nouvelle zone, cliquez sur **Add** (Ajouter). Pour modifier une zone existante, cliquez sur **Edit** (Modifier). Pour supprimer une zone sélectionnée, cliquez sur **Delete** (Supprimer).

La boîte de dialogue Add OSPFv3 Area (Ajouter une zone OSPFv3) ou Edit OSPFv3 Area (Modifier la zone OSPFv3) s'affiche.

Étape 4 Dans la liste déroulante OSPFv3 Process ID (ID de processus OSPFv3), choisissez l'ID de processus.

Étape 5 Saisissez l'ID de zone, qui spécifie la zone pour laquelle les routes doivent être résumées, dans le champ Area ID (ID de zone).

Étape 6 Choisissez le type de zone dans la liste déroulante Area Type (Type de zone). Les options disponibles sont Normal, NSSA et Stub.

Étape 7 Pour autoriser l'envoi de LSA récapitulatifs dans cette zone, cochez la case **Allow sending of summary LSAs into the area** (Autoriser l'envoi de LSA récapitulatifs dans la zone).

Étape 8 Pour autoriser la redistribution afin d'importer les routes vers les zones normales et non vers les zones stubby, cochez la case **Redistribution imports routes to normal and NSSA areas** (La redistribution importe les routes vers les zones normales et NSSA).

Étape 9 Pour générer une route externe par défaut dans un domaine de routage OSPFv3, cochez la case **Default information originate** (Origine des renseignements par défaut).

Étape 10 Saisissez la mesure utilisée pour générer la route par défaut dans le champ Metric (Mesure). La valeur par défaut est 10. Les valeurs de mesure valides sont comprises entre 0 et 16777214.

Étape 11 Dans la liste déroulante Metric Type (Type de mesure), choisissez le type de mesure. Le type de mesure est le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPFv3. Les options disponibles sont 1 pour un routage externe de type 1 ou 2 pour un routage externe de type 2.

Étape 12 Saisissez le coût dans le champ Default Cost (Coût par défaut).

Étape 13 Cliquez sur **OK**.

Étape 14 Cliquez sur l'onglet **Route Summarization** (Synthèse de routage).

Étape 15 Pour spécifier une nouvelle plage pour la consolidation et la synthèse des routes, cliquez sur **Add** (Ajouter). Pour modifier une plage existante pour la consolidation et la synthèse des routes, cliquez sur **Edit** (Modifier).

La boîte de dialogue Add Route Summarization (Ajouter une synthèse de routage) ou Edit Route Summarization (Modifier la synthèse de routage) s'affiche.

Étape 16 Dans la liste déroulante Process ID (ID de processus), choisissez l'ID de processus.

Étape 17 Dans la liste déroulante Area ID (ID de zone), choisissez l'ID de zone.

Étape 18 Saisissez le préfixe IPv6 et la longueur du préfixe dans le champ IPv6 Prefix/Prefix Length (Préfixe IPv6/Longueur du préfixe).

Étape 19 (Facultatif) Saisissez la mesure ou le coût de la route récapitulative, qui est utilisé lors des calculs de SPF OSPF pour déterminer les chemins les plus courts vers la destination. Les valeurs valides sont comprises entre 0 et 16 77 77 2015.

Étape 20 Cochez la case **Advertised** (Annoncé) pour définir l'état de la plage d'adresses comme annoncé et générer un LSA récapitulatif de type 3.

Étape 21 Cliquez sur **OK**.

Étape 22 Pour continuer, consultez Configurer un voisin de lien virtuel, à la page 966.

Configurer un voisin de lien virtuel

Pour configurer un voisin de lien virtuel, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Virtual Link (Liaison virtuelle)**.

Étape 2 Pour ajouter un nouveau voisin de lien virtuel, cliquez sur **Add** (Ajouter). Pour modifier un voisin de lien virtuel existant, cliquez sur **Edit** (Modifier). Pour supprimer un voisin de lien virtuel sélectionné, cliquez sur **Delete** (Supprimer).

La boîte de dialogue Add Virtual Link (Ajouter un lien virtuel) ou Edit Virtual Link (Modifier le lien virtuel) apparaît.

Étape 3 Dans la liste déroulante Process ID (ID de processus), choisissez l'ID de processus.

Étape 4 Dans la liste déroulante Area ID (ID de zone), choisissez l'ID de zone.

Étape 5 Saisissez l'ID de routeur homologue (c'est-à-dire l'adresse IP) dans le champ Peer Router ID (ID de routeur homologue).

Étape 6 (Facultatif) Saisissez le nombre de sauts de sécurité TTL (durée de vie) sur un lien virtuel dans le champ TTL Security (Sécurité TTL). La valeur du nombre de sauts peut aller de 1 à 254.

Étape 7 Dans la zone Timers (Minuteries), saisissez la durée en secondes pendant laquelle les paquets Hello ne sont pas vus avant qu'un voisin n'indique que le routeur est en panne dans le champ Dead Interval (Intervalle mort). L'intervalle mort est un entier non signé. La valeur par défaut est quatre fois l'intervalle Hello, soit 40 secondes. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun. Les valeurs valides vont de 1 à 8 192.

Étape 8 Saisissez la durée en secondes entre les paquets Hello qui sont envoyés sur une interface dans le champ Hello Interval (Intervalle Hello). L'intervalle Hello est un entier non signé qui doit être annoncé dans les paquets Hello. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun. Les valeurs valides vont de 1 à 8 192. La valeur par défaut est 10.

Étape 9 Saisissez la durée en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface dans le champ Retransmit Interval (Intervalle de retransmission). L'intervalle de retransmission est le délai aller-retour prévu entre deux routeurs du réseau associé. La valeur doit être supérieure au délai aller-retour attendu et peut varier de 1 à 8 192. La valeur par défaut est égale à 5.

Étape 10 Saisissez la durée estimée en secondes qui est requise pour envoyer un paquet de mise à jour d'état de liaison sur l'interface dans le champ Transmit Delay (Délai de transmission). La valeur entière doit être supérieure à zéro. Les LSA dans le paquet de mise à jour ont leur propre âge incrémenté de cette quantité avant transmission. La plage de valeurs peut aller de 1 à 8 192. La valeur par défaut est 1.

Étape 11 Dans la zone Authentication (Authentification), cochez la case **Enable Authentication** (Activer l'authentification) pour activer l'authentification.

Étape 12 Saisissez l'indice de la politique de sécurité, qui doit être un nombre compris entre 256 et 4294967295, dans le champ Security Policy Index (Indice de la politique de sécurité).

Étape 13 Choisissez l'algorithme d'authentification dans la liste déroulante Authentication Algorithm (Algorithme d'authentification). Les valeurs prises en charge sont SHA-1 et MD5. Lorsque l'authentification MD5 est utilisée, la clé doit comporter 32 chiffres hexadécimaux (16 octets). Lorsque l'authentification SHA-1 est utilisée, la clé doit comporter 40 chiffres hexadécimaux (20 octets).

Étape 14 Saisissez la clé d'authentification dans le champ Authentication Key (Clé d'authentification). La clé doit inclure 32 caractères hexadécimaux.

Étape 15 Choisissez l'algorithme de chiffrement dans la liste déroulante Encryption Algorithm (Algorithme de chiffrement). Les valeurs prises en charge sont AES-CD, 3DES et DES. L'entrée NULL indique qu'il n'y a pas de chiffrement.

Étape 16 Saisissez la clé de chiffrement dans le champ Encryption Key (Clé de chiffrement).

Étape 17 Cliquez sur **OK**.

Étape 18 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer des interfaces passives OSPFv3

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPFv3 que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

Étape 4 La zone Passive Interfaces (Interfaces passives) vous permet d'activer le routage OSPFv3 passif sur une interface. Le routage passif aide à contrôler l'annonce des informations de routage OSPFv3 et désactive l'envoi et la réception des mises à jour de routage OSPFv3 sur une interface. Dans la zone Passive Interfaces (Interfaces passives), choisissez les paramètres suivants :

- Cochez la case **Global passive** (Passif global) pour rendre passives toutes les interfaces répertoriées dans le tableau. Décochez des interfaces individuelles pour les rendre non passives.
- Décochez la case **Global passive** (Passif global) pour rendre toutes les interfaces non passives. Vérifiez les interfaces individuelles pour les rendre passives.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer la distance administrative OSPFv3

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

La zone Administrative Route Distances (Distances de routage administratif) vous permet de modifier les paramètres qui ont été utilisés pour configurer les distances de routage administratif. La distance de routage administratif doit être un entier compris entre 10 et 254. Dans la zone Administrative Route Distances (Distances de routage administratif), saisissez les valeurs suivantes :

- La valeur inter-zone, qui spécifie les routes inter-zone pour OSPV pour les routes IPv6.
- La valeur intra-zone, qui spécifie les routes intra-zone pour OSPF pour les routes IPv6.
- La valeur externe, qui spécifie les routes externes de type 5 et de type 7 pour OSPF pour les routes IPv6.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer les minuteries mOSPFv3

Vous pouvez définir les minuteries d'arrivée des LSA, de cadence des LSA et de limitation pour le protocole OSPFv3.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPFv3 que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

Étape 4 La zone Timer (Minuterie) vous permet de modifier les paramètres utilisés pour configurer l'arrivée des LSA, la cadence des LSA, la retransmission des LSA, la limitation des LSA et les heures de limitation SPF. Dans la zone Timers (Minuteries), saisissez les valeurs suivantes :

- L'arrivée de LSA, qui spécifie le délai minimum en millisecondes qui doit s'écouler entre l'acceptation de la même LSA provenant des voisins. La plage va de 100 à 1 000 millisecondes. La valeur par défaut est de 1 000 millisecondes.
- Le rythme de débordement de LSA, qui spécifie le temps en millisecondes auquel les LSA de la file d'attente de débordement sont cadencés entre les mises à jour. La plage configurable va de 5 à 100 millisecondes. La valeur par défaut est de 33 millisecondes.
- La cadence du groupe de LSA, qui spécifie l'intervalle en secondes auquel les LSA sont collectés dans un groupe et actualisés, additionnés ou rendus obsolètes. Les valeurs valides vont de 10 à 1 800. La valeur par défaut est 240.
- La cadence de retransmission de LSA, qui spécifie le temps en millisecondes auquel les LSA de la file d'attente de retransmission sont cadencés. La plage configurable va de 5 à 200 millisecondes. La valeur par défaut est de 66 millisecondes.
- La limitation initiale de LSA, qui spécifie le délai en millisecondes pour générer la première occurrence de LSA. La valeur par défaut est de 0 millisecondes.
- Le délai min. de limitation LSA, qui spécifie le délai minimum en millisecondes pour générer le même LSA. La valeur par défaut est de 5000 millisecondes.
- Le délai d'attente max. de la limitation LSA, qui spécifie le délai maximum en millisecondes pour générer le même LSA. La valeur par défaut est de 5000 millisecondes.

Remarque Pour la limitation des LSA, si la durée minimale ou maximale est inférieure à la valeur de première occurrence, OSPFv3 corrige automatiquement cette valeur de première occurrence. De même, si le délai maximal spécifié est inférieur au délai minimal, OSPFv3 corrige automatiquement à la valeur de délai minimal.

- La limitation SPF initiale, qui spécifie le délai en millisecondes avant de recevoir une modification du calcul SPF. La valeur par défaut est de 5000 millisecondes.

- Le délai min. de limitation SPF, qui spécifie le délai en millisecondes entre le premier et le deuxième calcul SPF. La valeur par défaut est de 10 000 millisecondes.
- Le délai d'attente max. de la limitation SPF, qui spécifie le temps d'attente maximum en millisecondes pour les calculs SPF. La valeur par défaut est de 10 000 millisecondes.

Remarque Pour la limitation SPF, si la durée minimale ou maximale est inférieure à la valeur de première occurrence, OSPFv3 corrige automatiquement la valeur de première occurrence. De même, si le délai maximal spécifié est inférieur au délai minimal, OSPFv3 corrige automatiquement à la valeur de délai minimal.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Définir les voisins OSPFv3 statiques

Vous devez définir des voisins OSPFv3 statiques pour annoncer les routes OSPF sur un réseau point à point de non-diffusion. Cette fonctionnalité vous permet de diffuser des annonces OSPFv3 sur une connexion VPN existante sans avoir à encapsuler les annonces dans un tunnel GRE.

Avant de commencer, vous devez créer une route statique vers le voisin OSPFv3. Consultez Configurer une route statique, à la page 867 pour en savoir plus sur la création des routes statiques.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Static Neighbor (Voisin statique)**.

Étape 2 Cliquez sur **Add** ou **Edit** (ajouter ou modifier) .

La boîte de dialogue Add or Edit Static Neighbor (Ajouter ou modifier un voisin statique) s'affiche. Cette boîte de dialogue vous permet de définir un nouveau voisin statique ou de modifier les renseignements d'un voisin statique existant. Vous devez définir un voisin statique pour chaque interface point à point de non-diffusion. Notez les restrictions suivantes :

- Vous ne pouvez pas définir le même voisin statique pour deux processus OSPFv3 différents.
- Vous devez définir une route statique pour chaque voisin statique.

Étape 3 Dans la liste déroulante Interface, choisissez l'interface associée au voisin statique. Si vous modifiez un voisin statique existant, vous ne pouvez pas modifier cette valeur.

Étape 4 Dans le champ Link-local Address (Adresse Link-Local), saisissez l'adresse IPv6 du voisin statique.

Étape 5 (Facultatif) Dans le champ Priority (Priorité), saisissez le niveau de priorité.

Étape 6 (Facultatif) Dans le champ Poll Interval (Intervalle entre interrogations), saisissez l'intervalle entre interrogations en secondes.

Étape 7 Cliquez sur **OK**.

Envoyer les messages du journal système

Configurez le routeur pour envoyer un message de journal système lorsqu'un voisin OSPFv3 est actif ou inactif.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

La zone Adjacency Changes (Modifications de contiguïté) vous permet de modifier les paramètres d'envoi de messages du journal système lorsqu'un voisin OSPFv3 est activé ou désactivé. Dans la zone Adjacency Changes (Modifications de contiguïté), procédez comme suit :

- Pour envoyer un message de journal système lorsqu'un voisin OSPFv3 est activé ou désactivé, cochez la case **Log Adjacency Changes** (Enregistrer les modifications de contiguïté).
- Pour envoyer un message de journal système pour chaque état, pas seulement lorsqu'un voisin OSPFv3 est activé ou désactivé, cochez la case **Include Details** (Inclure les détails).

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Apply** pour enregistrer vos modifications.

Supprimer les messages du journal système

Pour supprimer l'envoi des messages de journal système lorsque la route reçoit des paquets LSA de type 6 OSPF multidiffusion (MOSPF) non pris en charge, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPFv3 que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

Étape 4 Cochez la case **Ignore LSA MOSPF** (Ignorer LSA MOSPF), puis cliquez sur **OK**.

Calculer les coûts récapitulatifs de la route

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

Étape 4 Cochez la case **RFC1583 Compatible** (Compatible avec RFC 1583), puis cliquez sur **OK**.

Générer une route externe par défaut dans un domaine de routage OSPFv3

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPFv3 que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

Étape 4 Dans la zone Default Information Originate (Origine des renseignements par défaut), procédez comme suit :

a) Cochez la case **Enable** (Activer) pour activer le processus de routage OSPFv3.

b) Cochez la case **Always advertise** (Toujours annoncer) pour annoncer toujours la route par défaut, qu'elle existe ou non.

c) Saisissez la mesure utilisée pour générer la route par défaut dans le champ Metric (Mesure). Les valeurs de mesure valides sont comprises entre 0 et 16777214. La valeur par défaut est 10.

d) Dans la liste déroulante Metric Type (Type de métrique), choisissez le type de liaison externe associé à la route par défaut annoncée dans le domaine de routage OSPFv3. Les valeurs valides sont les suivantes :

- 1. Route externe de type 1
- 2. Route externe de type 2

La valeur par défaut est la route externe de type 2.

e) Dans la liste déroulante Route Map (Carte de routage), choisissez le processus de routage qui génère la route par défaut si la carte de routage est satisfaite.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer un préfixe de résumé IPv6

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Summary Prefix (Préfixe de résumé)**.

Étape 2 Pour ajouter un nouveau préfixe de résumé, cliquez sur **Add** (Ajouter). Pour modifier un préfixe de résumé existant, cliquez sur **Edit** (Modifier). Pour supprimer un préfixe de résumé, cliquez sur **Delete** (Supprimer).

La boîte de dialogue Add Summary Prefix (Ajouter un préfixe de résumé) ou Edit Summary Prefix (Modifier le préfixe de résumé) s'affiche.

Étape 3 Dans la liste déroulante Process ID (ID de processus), choisissez l'ID de processus.

Étape 4 Saisissez le préfixe IPv6 et la longueur du préfixe dans le champ IPv6 Prefix/Prefix Length (Préfixe IPv6/Longueur du préfixe).

Étape 5 Cochez la case **Advertise** (Annoncer) pour annoncer les routes qui correspondent à la paire préfixe-masque spécifiée. Décochez cette case pour supprimer les routages qui correspondent à la paire préfixe-masque spécifiée.

Étape 6 Dans le champ Tag (Balise), saisissez la valeur de balise que vous pouvez utiliser comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** pour enregistrer vos modifications.

Redistribuer les routes IPv6

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Redistribution**.

Étape 2 Pour ajouter de nouveaux paramètres afin de redistribuer les routes connectées dans un processus OSPFv3, cliquez sur **Add** (Ajouter). Pour modifier les paramètres existants afin de redistribuer les routes connectées dans un processus OSPFv3, cliquez sur **Edit** (Modifier). Pour supprimer un ensemble de paramètres sélectionné, cliquez sur **Delete** (Supprimer).

La boîte de dialogue Add Redistribution (Ajouter une redistribution) ou Edit Redistribution (Modifier la redistribution) s'affiche.

Étape 3 Dans la liste déroulante Process ID (ID de processus), choisissez l'ID de processus.

Étape 4 Dans la liste déroulante Source Protocol (Protocole source), choisissez le protocole source à partir duquel les routes sont redistribuées. Les protocoles pris en charge sont ceux qui sont connectés, statiques et OSPF.

Étape 5 Saisissez la valeur de mesure dans le champ Metric (Mesure). Lors de la redistribution de routes d'un processus OSPF dans un autre processus OSPF sur le même routeur, la mesure est transmise d'un processus à l'autre si aucune valeur de mesure n'est spécifiée. Lors de la redistribution d'autres processus dans un processus OSPF, la mesure par défaut est 20 lorsqu'aucune valeur de mesure n'est spécifiée.

Étape 6 Dans la liste déroulante Metric Type (Type de mesure), choisissez le type de mesure. Les options disponibles sont Aucune, 1 et 2.

Étape 7 (Facultatif) Saisissez la valeur de la balise dans le champ Tag (Balise). Ce paramètre spécifie la valeur décimale de 32 bits associée à chaque route externe, qui peut être utilisée pour communiquer des informations entre ASBR. Si aucune valeur n'est spécifiée, le numéro du système autonome distant est utilisé pour les routages de BGP et EGP. Pour les autres protocoles, zéro est utilisé. Les valeurs valides sont comprises entre 0 et 4294967295.

Étape 8 Choisissez la carte de routage à partir de la liste déroulante Route Map (Carte de routage) pour vérifier le filtrage de l'importation des routes du protocole de routage source au protocole de routage actuel. Si ce paramètre n'est pas spécifié, toutes les routes sont redistribuées. Si ce paramètre est spécifié, mais qu'aucune étiquette de carte de routage n'est répertoriée, aucune route n'est importée.

Étape 9 Pour inclure les routes connectées dans la redistribution, cochez la case **Include connected** (Inclure les routes connectées).

Étape 10 Cochez la case **Match** (Correspondance) pour redistribuer les routes dans d'autres domaines de routage, puis cochez l'une des cases suivantes :

- **Internal** (Interne) pour les routages internes à un système autonome spécifique
- **External 1** (Externe 1) pour les routes externes au système autonome, mais importées dans OSPFv3 en tant que routes externes de type 1
- **External 2** (Externe 2) pour les routes externes au système autonome, mais importées dans OSPFv3 en tant que routes externes de type 2
- **NSSA External 1** (NSSA Exerne 1) pour les routes externes au système autonome, mais importées dans OSPFv3 dans une NSSA pour IPv6 en tant que routes externes de type 1
- **NSSA External 2** (NSSA Externe 2) pour les routes externes au système autonome, mais importées dans OSPFv3 dans une NSSA pour IPv6 en tant que routes externes de type 2

Étape 11 Cliquez sur **OK**.

Étape 12 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer le redémarrage progressif

L'ASA peut connaître des situations de défaillance connues qui ne devraient pas affecter le transfert de paquets sur la plateforme de commutation. La capacité de transfert sans arrêt (NSF) permet au transfert de données de se poursuivre le long des routes connues, pendant la restauration des informations du protocole de routage.

En mode de haute disponibilité, le processus OSPF redémarre lorsque l'unité active devient inactive et que l'unité en veille devient la nouvelle active. De même, en mode grappe, le processus OSPF redémarre lorsque l'unité de contrôle devient inactive et que l'unité de données est choisie comme nouvelle unité de contrôle. Ces processus de transition OSPF entraînent un retard considérable. Vous pouvez configurer NSF pour éviter

la perte de trafic lors du changement d'état du processus OSPF. La fonctionnalité NSF est également utile lorsqu'une mise à niveau logicielle rapide est planifiée.

Le redémarrage progressif est pris en charge sur les protocoles OSPFv2 et OSPFv3. Vous pouvez configurer le redémarrage progressif sur OSPFv2 en utilisant NSF IETF (RFC 3623). Vous pouvez configurer le redémarrage progressif sur OSPFv3 à l'aide du redémarrage progressif (RFC 5187).

La configuration de la fonction de redémarrage progressif NSF comporte deux étapes : la configuration des capacités et la configuration d'un périphérique compatible avec NSF ou conscient de NSF. Un périphérique compatible NSF peut indiquer ses propres activités de redémarrage aux voisins, et il peut aider un voisin qui redémarre.

Un périphérique peut être configuré comme compatible NSF ou comme conscient de NSF, selon certaines conditions :

- Un périphérique peut être configuré comme compatible NSF, quel que soit le mode dans lequel il se trouve.
- Un périphérique doit être en mode de basculement ou de grappe EtherChannel étendu (L2) pour être configuré comme compatible NSF.
- Pour qu'un périphérique soit compatible NSF ou conscient de NSF, il doit être configuré de manière à traiter les blocs couvrant les publicités d'état de liaison (LSA) opaques et les signalisations locales de liaison (LLS), selon les besoins.

Remarque Lorsque des Hello rapides sont configurés pour le protocole OSPFv2, le redémarrage progressif ne se produit pas lorsque l'unité active est rechargée et que l'unité en veille devient active. En effet, le temps nécessaire au changement de rôle est supérieur à l'intervalle de temps mort configuré.

Configuration du redémarrage progressif pour OSPFv2

Il existe deux mécanismes de redémarrage progressif pour OSPFv2, Cisco NSF et IETF NSF. Un seul de ces mécanismes de redémarrage progressif peut être configuré à la fois pour une instance ospf. Un périphérique conscient de NSF peut être configuré à la fois comme assistant NSF Cisco et comme assistant NSF IETF, mais un périphérique compatible avec NSF peut être configuré en mode Cisco NSF ou IETF NSF à la fois pour une instance ospf.

Configurer le redémarrage progressif de Cisco NSF pour OSPFv2

Configurez le redémarrage progressif de Cisco NSF pour OSPFv2, pour un périphérique compatible avec NSF ou conscient de NSF.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Setup (Configuration) > Advanced (Avancé) > Add NSF Properties (Ajouter des propriétés NSF).

Étape 2 Sous Configuring Cisco NSF (Configuration de Cisco NSF), cochez la case Enable Cisco nonstop forwarding (NSF) (Activer le transfert sans arrêt Cisco (NSF)).

Étape 3 (Facultatif) Cochez la case Cancels NSF restart when non-NSF-aware neighboring networking devices are detected (Annuler le redémarrage de NSF lorsque des appareils réseau voisins non sensibles à NSF sont détectés), le cas échéant.

Étape 4 (Facultatif) Sous Configuring Cisco NSF helper (Configuration de l'assistance Cisco NSF), décochez la case Enable Cisco nonstop forwarding (NSF) (Activer le transfert sans arrêt Cisco (NSF)) pour le mode d'assistance.

Remarque Cette option est cochée par défaut. Décochez cette case pour désactiver le mode d'assistance Cisco NSF sur un périphérique conscient de NSF.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Configuration de la minuterie d'attente de redémarrage progressif pour le OSPF

Configurez le redémarrage progressif IETF NSF pour OSPFv2, pour un périphérique compatible avec NSF ou conscient de NSF.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Setup (Configuration) > Advanced (Avancé) > Add NSF Properties (Ajouter des propriétés NSF)**.

Étape 2 Sous Configuring IETF NSF (Configuration IETF NSF), cochez la case Enable IETF nonstop forwarding (NSF) (Activer le transfert sans arrêt IETF (NSF)).

Étape 3 (Facultatif) Entrez l'intervalle de redémarrage en secondes dans le champ Length of graceful restart interval (Durée de l'intervalle de redémarrage progressif).

Remarque La valeur par défaut est 120secondes. Pour un intervalle de redémarrage inférieur à 30 secondes, le redémarrage progressif sera interrompu.

Étape 4 (Facultatif) Sous Configuring IETF NSF helper (Configuration de l'assistance IETF NSF), décochez la case Enable IETF nonstop forwarding (NSF) (Activer le transfert sans arrêt IETF (NSF)) pour le mode d'assistance.

Cette option est cochée par défaut. Décochez cette case pour désactiver le mode d'assistance IETF NSF sur un périphérique conscient de NSF.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Configuration du redémarrage progressif pour OSPFv3

La configuration de la fonctionnalité de redémarrage progressif NSF pour OSPFv3 comporte deux étapes : la configuration d'un périphérique pour qu'il soit compatible NSF, puis la configuration d'un périphérique pour qu'il soit conscient de NSF.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Setup (Configuration) > Advanced (Avancé) > Add NSF Properties (Ajouter des propriétés NSF)**.

Étape 2 Sous Configuring Graceful Restart (Configuration du redémarrage progressif), cochez la case Enable Graceful Restart (Activer le redémarrage progressif).

Étape 3 (Facultatif) Saisissez une valeur pour l'intervalle de redémarrage dans le champ Restart Interval (Intervalle de redémarrage).

Remarque La valeur par défaut est 120secondes. Pour un intervalle de redémarrage inférieur à 30 secondes, le redémarrage progressif sera interrompu.

Étape 4 Sous Configuring Graceful Restart Helper (Configuration de l'assistance au redémarrage progressif), cochez la case Enable Graceful Restart Helper (Activer l'assistance au redémarrage progressif).

Cette option est cochée par défaut. Décochez cette case pour désactiver le mode d'assistance au redémarrage progressif sur un périphérique compatible avec NSF.

Étape 5 (Facultatif) Cochez la case Enable LSA (Activer LSA) pour activer la vérification stricte des déclarations de l'état des liens.

Lorsqu'elle est cochée, elle indique que le routeur d'assistance mettra fin au processus de redémarrage du routeur s'il détecte une modification d'un LSA qui serait débordé vers le routeur qui redémarre, ou si un LSA modifié figure sur la liste de retransmission du routeur qui redémarre lorsque le processus de redémarrage progressif est lancé.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Apply** pour enregistrer vos modifications.

Configuration de la minuterie d'attente de redémarrage progressif pour OSPF

On s'attend à ce que les routeurs OSPF définissent le bit RS dans l'EO-TLV associé à un paquet Hello lorsqu'on ne sait pas que tous les voisins sont répertoriés dans le paquet, mais que les routeurs qui redémarrent doivent conserver leurs contiguïtés. Cependant, la valeur du bit RS ne doit pas être supérieure aux secondes de RouterDeadInterval. Par conséquent, la commande **timers nsf wait** est introduite pour définir le bit RS dans les paquets Hello inférieurs aux secondes de RouterDeadInterval. La valeur par défaut de la minuterie d'attente de NSF est de 20 secondes.

Avant de commencer

- Pour configurer le délai d'attente de Cisco NSF pour OSPF, le périphérique doit être conscient de NSF ou compatible avec NSF.

Procédure

Étape 1 Entrez en mode de configuration du routeur OSPF.

Exemple :

```
ciscoasa(config)# router ospf
```

Étape 2 Entrez les minuteries et spécifiez nsf.

Exemple :

```
ciscoasa(config-router)# timers?
router mode commands/options:
  lsa       OSPF LSA timers
  nsf       OSPF NSF timer
  pacing    OSPF pacing timers
  throttle  OSPF throttle timers
ciscoasa(config-router)# timers nsf ?
```

Étape 3 Saisissez l'intervalle d'attente du redémarrage progressif. Cette valeur peut être comprise entre 1 et 65 535.

Exemple :

```
ciscoasa(config-router)# timers nsf wait 200
```

En utilisant l'intervalle d'attente du redémarrage progressif, vous pouvez vous assurer que l'intervalle d'attente n'est pas supérieur à l'intervalle de temps mort du routeur.

Supprimer la configuration OSPFv2

Supprimez la configuration OSPFv2.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Décochez la case **Enable this OSPF Process** (Activer ce processus OSPF).

Étape 3 Cliquez sur **Apply** (Appliquer).

Supprimer la configuration OSPFv3

Supprimez la configuration OSPFv3.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Décochez la case **Enable this OSPFv3 Process** (Activer ce processus OSPFv3).

Étape 3 Cliquez sur **Apply** (Appliquer).

Exemple de protocole OSPFv2

L'exemple suivant montre comment activer et configurer le protocole OSPFv2 avec différents processus facultatifs :

1. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.
2. Cliquez sur l'onglet **Process Instances** (Instances de processus) et dans le champ OSPF Process 1 (Processus 1 d'OSPF), tapez **2**.
3. Cliquez sur l'onglet **Area/Networks** (Zone/Réseaux), puis cliquez sur **Add** (Ajouter).
4. Saisissez **0** dans le champ Area ID (ID de zone).
5. Dans la zone Area Networks (Réseaux de zone), saisissez **10.0.0.0** dans le champ IP Address (Adresse IP).
6. Sélectionnez 255.0.0.0 dans la liste déroulante Netmask (Masque réseau).
7. Cliquez sur **OK**.
8. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Redistribution**.
9. Cliquez sur **Add** (ajouter).

   La boîte de dialogue Add/Edit OSPF Redistribution Entry (Ajouter/modifier une entrée de redistribution OSPF) apparaît.
10. Dans la zone Protocol (Protocole), cliquez sur le bouton radio **OSPF** pour choisir le protocole source à partir duquel les routes sont redistribuées. Choisir OSPF redistribue les routes à partir d'un autre processus de routage OSPF.
11. Choisissez l'ID de processus OSPF dans la liste déroulante OSPF Process (Processus OSPF).
12. Dans la zone Match (Correspondance), cochez la case **Internal** (Interne).
13. Dans le champ Metric Value (Valeur de la mesure), saisissez **5** pour la valeur de mesure des routes redistribuées.
14. Dans la liste déroulante Metric Type (Type de mesure), choisissez 1 pour la valeur de type de mesure.
15. Dans la liste déroulante Route Map (Carte de routage), choisissez 1.

16. Cliquez sur **OK**.
17. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Interface**.
18. Dans l'onglet Properties (Propriétés), choisissez l'interface **inside** (interne) et cliquez sur **Edit** (Modifier).

    La boîte de dialogue Edit OSPF Properties (Modifier les propriétés OSPF) apparaît.
19. Dans le champ Cost (Coût), saisissez **20**.
20. Cliquez sur **Advanced** (Avancé).
21. Dans le champ Retransmit Interval (Intervalle de retransmission), saisissez **15**.
22. Dans le champ Transmit Delay (Délai de transmission), saisissez **20**.
23. Dans le champ Hello Interval (Intervalle Hello), saisissez **10**.
24. Dans le champ Dead Interval (Intervalle de temps mort), saisissez **40**.
25. Cliquez sur **OK**.
26. Dans la boîte de dialogue Edit OSPF Properties (Modifier les propriétés OSPF), saisissez **20** dans le champ Properties (Priorités), puis cliquez sur **OK**.
27. Cliquez sur l'onglet **Authentication** (Authentification).

    La boîte de dialogue Edit OSPF Authentication (Modifier l'authentification OSPF) s'affiche.
28. Dans la zone Authentication (Authentification), cliquez sur le bouton radio **MD5**.
29. Dans la zone MD5 and Key ID (ID de clé), saisissez **cisco** dans le champ MD5 Key (Clé MD5) et **1** dans le champ MD5 Key ID (ID de clé MD5).
30. Cliquez sur **OK**.
31. Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**, puis cliquez sur l'onglet **Area/Networks** (Zone/Réseaux).
32. Choisissez le processus **OSPF 2** et cliquez sur **Edit** (Modifier).

    La boîte de dialogue Edit OSPF Area (Modifier une zone OSPF) apparaît.
33. Dans la zone Area Type (Type de zone), choisissez **Stub**.
34. Dans la zone Authentication (Authentification), choisissez **None** (Aucun), et saisissez **20** dans le champ Default Cost (Coût par défaut).
35. Cliquez sur **OK**.
36. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.
37. Cliquez sur l'onglet **Process Instances** (Instances de processus) et cochez la case **OSPF process 2** (Processus 2 d'OSPF).
38. Cliquez sur **Advanced** (Avancé).

    La boîte de dialogue Edit OSPF Area (Modifier une zone OSPF) apparaît.

39. Dans la zone Timers (Minuteries), saisissez **10** dans le champ SPF Delay Time (Délai d'attente SPF) et **20** dans le champ SPF Hold Time (Délai de rétention SPF).
40. Dans la zone Adjacency Changes (Modifications de contiguïté), cochez la case **Log Adjacency Change Details** (Journaliser les détails des modifications de contiguïté).
41. Cliquez sur **OK**.
42. Cliquez sur **Reset** (Réinitialiser).

Exemples de protocole OSPFv3

L'exemple suivant montre comment configurer le routage OSPFv3 dans ASDM :

1. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.
2. Sous l'onglet Process Instances (Instances de processus), procédez comme suit :
    1. Cochez la case **Enable this OSPFv3 Process** (Activer ce processus OSPFv3).
    2. Saisissez **1** dans le champ Process ID (ID de processus).
3. Cliquez sur l'onglet **Areas** (Zones), puis sur **Add** (Ajouter) pour afficher la boîte de dialogue Add OSPFv3 Area (Ajouter une zone OSPFv3).
4. Dans la liste déroulante OSPFv3 Process ID (ID de processus OSPFv3), choisissez **1**.
5. Saisissez **22** dans le champ Area ID (ID de zone).
6. Choisissez **Normal** dans la liste déroulante Area Type (Type de zone).
7. Saisissez **10** dans le champ Default Cost (Coût par défaut).
8. Cochez la case **Redistribution imports routes to normal and NSSA areas** (La redistribution importe les routes dans les zones normales et NSSA).
9. Saisissez **20** dans le champ Metric (Mesure).
10. Choisissez **1** dans la liste déroulante Metric Type (Type de mesure).
11. Cochez la case **inside** (interne) en tant qu'interface spécifiée.
12. Cochez la case **Enable Authentication** (Activer l'authentification).
13. Saisissez **300** dans le champ Security Policy Index (Indice de la politique de sécurité).
14. Choisissez **SHA-1** dans la liste déroulante Authentication Algorithm (Algorithme d'authentification).
15. Saisissez **12345ABCDE** dans le champ Authentication Key (Clé d'authentification).
16. Choisissez **DES** dans la liste déroulante Encryption Algorithm (Algorithme de chiffrement).
17. Saisissez **1122334455aabbccddee** dans le champ Encryption Key (Clé de chiffrement).
18. Cliquez sur **OK**.

19. Cliquez sur l'onglet **Route Summarization** (Synthèse du routage), puis sur **Add** (Ajouter) pour afficher la boîte de dialogue Add Route Summarization (Ajouter la synthèse du routage).
20. Choisissez **1** dans la liste déroulante Process ID (ID de processus).
21. Choisissez **22** dans la liste déroulante Area ID (ID de zone).
22. Saisissez **2000:122::/64** dans le champ IPv6 Prefix/Prefix Length (Préfixe IPv6/Longueur du préfixe).
23. (Facultatif) Saisissez **100** dans le champ Cost (Coût).
24. Cochez la case **Advertised** (Annoncé).
25. Cliquez sur **OK**.
26. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Interface**.
27. Cliquez sur l'onglet **Properties** (Propriétés).
28. Cochez la case **inside** (interne) et cliquez sur **Edit** (Modifier) pour afficher la boîte de dialogue Edit OSPF Properties (Modifier les propriétés OSPF).
29. Dans le champ Cost (Coût), saisissez **20**.
30. Saisissez **1** dans le champ Priority (Priorité).
31. Cochez la case **point-to-point** (point à point).
32. Dans le champ Dead Interval (Intervalle de temps mort), saisissez **40**.
33. Dans le champ Hello Interval (Intervalle Hello), saisissez **10**.
34. Dans le champ Retransmit Interval (Intervalle de retransmission), saisissez **15**.
35. Dans le champ Transmit Delay (Délai de transmission), saisissez **20**.
36. Cliquez sur **OK**.
37. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Redistribution**.
38. Choisissez **1** dans la liste déroulante Process ID (ID de processus).
39. Choisissez **OSPF** dans la liste déroulante Source Protocol (Protocole source).
40. Saisissez **50** dans le champ Metric (Mesure).
41. Choisissez **1** dans la liste déroulante Metric Type (Type de mesure).
42. Cliquez sur **OK**.
43. Cliquez sur **Apply** pour enregistrer vos modifications.

Supervision OSPF

Vous pouvez afficher des statistiques spécifiques, comme le contenu des tables de routage IP, des caches et des bases de données. Vous pouvez également utiliser les renseignements fournis pour déterminer l'utilisation

des ressources et résoudre les problèmes de réseau. Vous pouvez également afficher des renseignements sur l'accessibilité des nœuds et découvrir le chemin de routage emprunté par les paquets de votre périphérique à travers le réseau.

Pour superviser ou afficher diverses statistiques de routage OSPFv2 dans ASDM, procédez comme suit :

1. Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **OSPF LSAs (LSA OSPF)**.
2. Vous pouvez sélectionner et superviser les LSA OSPF de type 1 à 5 et 7. Chaque volet affiche un type de LSA, comme suit :
   - Les LSA de type 1 représentent les routes d'une zone en vertu d'un processus.
   - Les LSA de type 2 affichent l'adresse IP du routeur désigné qui annonce les routeurs.
   - Les LSA de type 3 affichent l'adresse IP du réseau de destination.
   - Les LSA de type 4 affichent l'adresse IP du routeur de limite AS.
   - Les LSA de type 5 et de type 7 affichent l'adresse IP du réseau externe de l'AS.
3. Cliquez sur **Refresh** (Actualiser) pour mettre à jour chaque volet de type LSA.
4. Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **OSPF Neighbors (Voisins OSPF)**.

   Dans le volet OSPF Neighbors (Voisins OSPF), chaque ligne représente un voisin OSPF. De plus, le volet OSPF Neighbors (Voisins OSPF) affiche le réseau sur lequel le voisin s'exécute, la priorité, l'état, la durée de temps mort en secondes, l'adresse IP du voisin et l'interface sur laquelle il s'exécute. Pour obtenir la liste des états possibles pour un voisin OSPF, consultez la RFC 2328.
5. Cliquez sur **Refresh** (Actualiser) pour mettre à jour le volet OSPF Neighbors (Voisins OSPF).

Pour superviser ou afficher diverses statistiques de routage OSPFv3 dans ASDM, procédez comme suit :

1. Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **OSPFv3 LSAs (LSA OSPFv3)**.
2. Vous pouvez sélectionner et superviser les LSA OSPFv3. Choisissez un type d'état de liaison pour afficher son état en fonction des paramètres spécifiés dans la liste déroulante Link State type (Type d'état de liaison). Les types d'états de liaison pris en charge sont les suivants : routeur, réseau, préfixe inter-zone, routeur inter-zone, AS externe, NSSA, liaison et préfixe intra-zone.
3. Cliquez sur **Refresh** (Actualiser) pour mettre à jour chaque type d'état de liaison.
4. Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **OSPFv3 Neighbors (Voisins OSPFv3)**.

   Dans le volet OSPFv3 Neighbors (Voisins OSPFv3), chaque ligne représente un voisin OSPFv3. De plus, le volet OSPFv3 Neighbors (Voisins OSPFv3) affiche l'adresse IP du voisin, la priorité, l'état, la durée de temps mort en secondes et l'interface sur laquelle il s'exécute. Pour obtenir la liste des états possibles pour un voisin OSPFv3, consultez la RFC 5340.
5. Cliquez sur **Refresh** (Actualiser) pour mettre à jour le volet OSPFv3 Neighbors (Voisins OSPFv3).

Historique OSPF

Tableau 42 : Historique des fonctionnalités OSPF

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge OSPF	7.0(1)	Une prise en charge a été ajoutée pour les données de routage, l'authentification, la redistribution et la supervision des informations de routage à l'aide du protocole de routage Open Shortest Path First (OSPF). Nous avons introduit l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF.
Routage dynamique en mode de contexte multiple	9.0(1)	Le routage OSPFv2 est pris en charge en mode de contexte multiple. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Setup (Configuration)
Mise en grappe	9.0(1)	Pour OSPFv2 et OSPFv3, la synchronisation groupée, la synchronisation du routage et l'équilibrage de charges EtherChannel étendu sont pris en charge dans l'environnement de mise en grappe.
Prise en charge OSPFv3 pour IPv6	9.0(1)	Le routage OSPFv3 est pris en charge pour IPv6. Nous avons introduit les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Setup, Configuration (Configuration) > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Interface, Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Redistribution, Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Summary Prefix (Préfixe du sommaire), Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Virtual Link, Monitoring (Lien virtuel, Supervision) > Routing (Routage) > OSPFv3 LSAs (LSA OSPFv3), Monitoring (Supervision) > Routing (Routage) > OSPFv3 Neighbors (Voisins OSPFv3).
Prise en charge OSPF pour les Hellos rapides	9.2(1)	OSPF prend en charge la fonctionnalité Paquets Hello rapides, ce qui permet d'obtenir une configuration qui accélère la convergence dans un réseau OSPF. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Interface > Edit OSPF Interface (Modifier les propriétés avancées de l'interface OSPF)
Minuteries	9.2(1)	De nouvelles minuteries OSPF ont été ajoutées; les anciennes ont été rendues obsolètes. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Setup (Configuration) > Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF)

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Filtrage des routes à l'aide de la liste d'accès	9.2(1)	Le filtrage des routes à l'aide d'ACL est désormais pris en charge. Nous avons introduit l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Filtering Rules (Règles de filtrage) > Add Filter Rules (Ajouter des règles de filtre)
Améliorations de la surveillance OSPF	9.2(1)	Des informations supplémentaires sur la surveillance OSPF ont été ajoutées.
OSPF redistribue le BGP	9.2(1)	La fonctionnalité de redistribution OSPF a été ajoutée. Nous avons ajouté l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Redistribution
Prise en charge OSPF pour la transmission sans interruption (NSF)	9.3(1)	La prise en charge des protocoles OSPFv2 et OSPFv3 pour NSF a été ajoutée. Nous avons ajouté les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Setup (Configuration) > NSF Properties (Propriétés du NSF), Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Setup (Configuration) > NSF Properties (Propriétés du NSF)
Prise en charge OSPF pour la transmission sans interruption (NSF)	9.13(1)	La minuterie d'attente NSF a été ajoutée. Nous avons ajouté une nouvelle commande pour définir la minuterie de l'intervalle de redémarrage NSF. Cette commande a été introduite pour s'assurer que l'intervalle d'attente n'est pas plus long que l'intervalle de temps mort du routeur. Nous avons introduit la commande suivante : **timers nsf wait <seconds>**



CHAPITRE 35

IS-IS

Ce chapitre décrit le protocole de routage IS-IS (Intermediate System to Intermediate System).

- À propos d'IS-IS, à la page 987
- Conditions préalables d'IS-IS, à la page 993
- Lignes directrices relatives à IS-IS, à la page 994
- Configurer IS-IS, à la page 994
- Supervision IS-IS, à la page 1012
- Historique d'IS-IS, à la page 1013

À propos d'IS-IS

Le protocole de routage IS-IS est un protocole IGP (Interior Gateway Protocol) à état de liaison. Les protocoles à état de liaison se caractérisent par la propagation des renseignements nécessaires pour créer une carte complète de la connectivité du réseau sur chaque périphérique participant. Cette carte est ensuite utilisée pour calculer le chemin le plus court vers les destinations. La mise en œuvre d'IS-IS prend en charge IPv4 et IPv6.

Vous pouvez diviser un domaine de routage en un ou plusieurs sous-domaines. Chaque sous-domaine est appelé une zone et se voit attribuer une adresse de zone. Le routage dans une zone est appelé routage de niveau 1. Le routage entre les zones de niveau 1 est appelé routage de niveau 2. Un routeur est appelé système intermédiaire (IS). Un IS peut fonctionner au niveau 1, au niveau 2 ou aux deux. Les IS qui fonctionnent au niveau 1 échangent des renseignements de routage avec d'autres IS de niveau 1 dans la même zone. Les IS qui fonctionnent au niveau 2 échangent des renseignements de routage avec d'autres routeurs de niveau 2, qu'ils se trouvent ou non dans la même zone de niveau 1. L'ensemble de routeurs de niveau 2 et les liaisons qui les relient forment le sous-domaine de niveau 2, qui ne doit pas être partitionné pour que le routage fonctionne correctement.

À propos de NET

Un IS est identifié par une adresse appelée Network Entity Title (NET). Le NET est l'adresse d'un point d'accès de service de réseau (NSAP), qui identifie une instance du protocole de routage IS-IS exécuté sur un IS. Le NET comporte de 8 à 20 octets et comprend les trois parties suivantes :

- Adresse de zone : ce champ a une longueur de 1 à 13 octets et est composé des octets de poids fort de l'adresse.

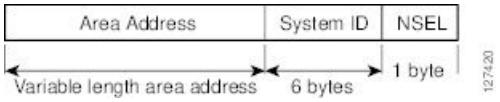
Remarque Vous pouvez attribuer plusieurs adresses de zone à une instance IS-IS; dans ce cas, toutes les adresses de zone sont considérées comme synonymes. Plusieurs adresses de zone synonymes sont utiles lors de la fusion ou de la division de zones dans le domaine. Une fois la fusion ou la division terminée, vous n'avez pas besoin d'attribuer plusieurs adresses de zone à une instance IS-IS.

- ID de système : ce champ a une longueur de 6 octets et suit immédiatement l'adresse de zone. Lorsque l'IS fonctionne au niveau 1, l'ID système doit être unique pour les périphériques de niveau 1 dans la même zone. Lorsque l'IS fonctionne au niveau 2, l'ID système doit être unique parmi tous les périphériques du domaine.

Remarque Vous attribuez un ID système à une instance IS.

- NSEL : le champ du sélecteur N a une longueur de 1 octet et suit immédiatement l'ID système. Il doit être défini sur 00.

Illustration 84 : Format NET



Nom de domaine dynamique IS-IS

Dans le domaine de routage IS-IS, l'ID système est utilisé pour représenter chaque ASA. L'ID système fait partie du NET configuré pour chaque ASA IS-IS. Par exemple, un ASA avec un NET configuré de 49.0001.0023.0003.000a.00 a un ID système de 0023.0003.000a. Le mappage du nom de l'ASA à l'ID système est difficile à mémoriser pour les administrateurs réseau lors de la maintenance et de la résolution des problèmes des ASA.

Le mécanisme de nom d'hôte dynamique utilise le protocole LSP (Link State Protocol) pour distribuer les renseignements de mappage du nom de l'ASA à l'ID système sur l'ensemble du réseau. Chaque ASA du réseau tentera d'installer les renseignements de mappage de l'ID système au nom de l'ASA dans sa table de routage.

Si un ASA qui a annoncé le type de nom dynamique, la longueur et la valeur (TLV) sur le réseau cesse soudainement l'annonce, les derniers renseignements de mappage reçus resteront dans le tableau de mappage de l'hôte dynamique pendant une heure maximum, ce qui permettra à l'administrateur réseau d'afficher les entrées du tableau de mappage à un moment où le réseau rencontre des problèmes.

Types de PDU IS-IS

Les IS échangent des renseignements de routage avec leurs homologues à l'aide d'unités de données de protocole (PDU). Les types de PDU Hello Intermediate System-to-Intermediate System (IIH), de PDU d'état de liaison (LSP) et de PDU de numéro de séquence (SNP) sont utilisés.

IIH

Les IIH sont échangés entre les voisins IS sur les circuits sur lesquels le protocole IS-IS est activé. Les IIH comprennent l'ID système de l'expéditeur, la ou les adresses de zone attribuées et l'identité des voisins sur ce circuit connus de l'IS expéditeur. Des renseignements facultatifs supplémentaires peuvent également être inclus.

Il existe deux types d'IIH :

- IIH LAN de niveau 1 : ceux-ci sont envoyés sur les circuits multiaccès lorsque l'IS d'envoi fonctionne comme un appareil de niveau 1 sur ce circuit.
- IIH LAN de niveau 2 : ceux-ci sont envoyés sur les circuits multiaccès lorsque l'IS d'envoi fonctionne comme un appareil de niveau 2 sur ce circuit.

LSP

Un IS génère des LSP pour annoncer ses voisins et les destinations qui sont directement connectées à cet IS. Un LSP est identifié de façon unique par les éléments suivants :

- ID de système de l'IS qui a généré le LSP
- ID de pseudo-nœud : cette valeur est toujours égale à 0, sauf lorsque le LSP est un LSP de pseudo-nœud.
- Numéro LSP (0 à 255)
- Numéro de séquence de 32 bits

Chaque fois qu'une nouvelle version d'un LSP est générée, le numéro de séquence est incrémenté.

Les LSP de niveau 1 sont générés par les IS qui prennent en charge le niveau 1. Les LSP de niveau 1 sont inondés dans toute la zone de niveau 1. L'ensemble de LSP de niveau 1 généré par tous les IS de niveau 1 d'une zone constitue la base de données LSP de niveau 1 (LSPDB). Tous les IS de niveau 1 d'une zone ont une LSPDB de niveau 1 identique et, par conséquent, une carte de connectivité réseau identique pour la zone.

Les LSP de niveau 2 sont générés par les IS qui prennent en charge le niveau 2. Les LSP de niveau 2 sont inondés dans tout le sous-domaine de niveau 2. L'ensemble de LSP de niveau 2 généré par tous les IS de niveau 2 du domaine constitue la base de données LSP de niveau 2 (LSPDB). Tous les IS de niveau 2 ont une LSPDB de niveau 2 identique et, par conséquent, une carte de connectivité identique pour le sous-domaine de niveau 2.

SNP

Les SNP contiennent une description sommaire d'un ou de plusieurs LSP. Il existe deux types de SNP pour les niveaux 1 et 2 :

- Les PDU à numéro de séquence complet (CSNP) sont utilisées pour envoyer un résumé de la base de données LSPDB dont dispose un IS pour un niveau donné.
- Les PDU à numéro de séquence partiel (PSNP) sont utilisées pour envoyer un résumé d'un sous-ensemble des LSP pour un niveau donné qu'un IS possède dans sa base de données ou doit obtenir.

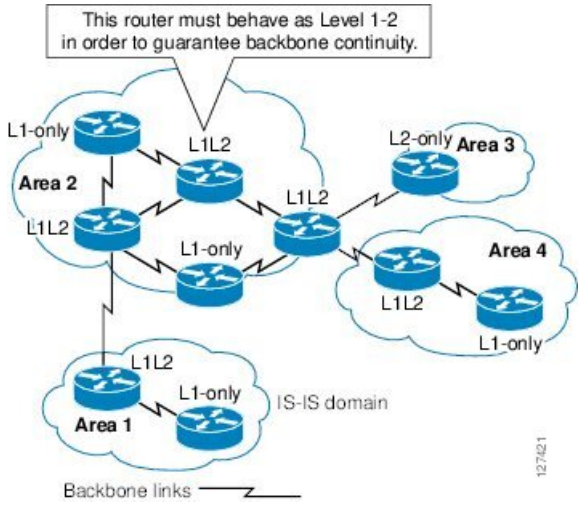
Fonctionnement d'IS-IS sur les circuits multiaccès

Les circuits multiaccès prennent en charge plusieurs IS, c'est-à-dire deux ou plus fonctionnant sur le circuit. Pour les circuits multiaccès, une condition préalable nécessaire est la capacité d'adresser plusieurs systèmes à l'aide d'une adresse de multidiffusion ou de diffusion. Un IS qui prend en charge le niveau 1 sur un circuit multiaccès envoie des IIH de niveau 1 LAN sur le circuit. Un IS qui prend en charge le niveau 2 sur un circuit multiaccès envoie des IIH LAN de niveau 2 sur le circuit. Les IS forment des contiguïtés distinctes pour chaque niveau avec les IS voisins sur le circuit.

Un IS forme une contiguïté de niveau 1 avec d'autres IS qui prennent en charge le niveau 1 sur le circuit et qui ont une adresse de zone correspondante. Deux ISE avec des ensembles dissociés d'adresses de zone prenant en charge le niveau 1 sur le même circuit multiaccès ne sont PAS pris en charge. Un IS forme une contiguïté de niveau 2 avec d'autres IS qui prennent en charge le niveau 2 sur le circuit.

Les périphériques de la topologie du réseau IS-IS dans la figure suivante effectuent le routage de niveau 1, de niveau 2 ou de niveau 1 et 2 le long du réseau fédérateur.

Illustration 85 : Périphériques de niveau 1, de niveau 2 et de niveau 1-2 dans une topologie de réseau IS-IS



Choix de l'IS désigné IS-IS

Si chaque IS annonce toutes ses contiguïtés sur un circuit de multiaccès dans ses LSP, le nombre total d'annonces requis serait de N 2 (où N est le nombre d'ISE qui fonctionnent à un niveau donné sur le circuit). Pour résoudre ce problème d'évolutivité, IS-IS définit un pseudo-nœud pour représenter le circuit de multiaccès. Tous les IS qui fonctionnent sur le circuit à un niveau donné choisissent un des IS pour qu'il agisse en tant que système intermédiaire désigné (DIS) sur ce circuit. Un DIS est choisi pour chaque niveau actif sur le circuit.

Le DIS est responsable de l'émission de LSP de pseudo-nœuds. Les LSP de pseudo-nœuds comprennent des annonces de voisins pour tous les IS qui fonctionnent sur ce circuit. Tous les IS qui fonctionnent sur le circuit (y compris le DIS) fournissent une annonce de voisin au pseudo-nœud dans leurs LSP non pseudo-nœuds et n'annoncent aucun de leurs voisins sur le circuit de multiaccès. De cette façon, le nombre total d'annonces requises varie en fonction du N, le nombre d'ISE qui fonctionnent sur le circuit.

Un LSP de pseudo-nœud est classifié de manière unique par les identifiants suivants :

- ID de système du DIS qui a généré le LSP

- Identifiant de pseudo-nœud (TOUJOURS NON ZÉRO)
- Numéro LSP (0 à 255)
- Numéro de séquence de 32 bits

L'ID de pseudo-nœud non zéro est ce qui différencie un LSP de pseudo-nœud d'un LSP non pseudo-nœud. Il est choisi par le DIS pour être unique parmi tous les autres circuits LAN pour lesquels il est également le DIS à ce niveau.

Le DIS est également responsable de l'envoi des CSNP périodiques sur le circuit. Cela fournit une description complète du contenu actuel de la LSPDB sur le DIS. D'autres IS sur le circuit peuvent alors effectuer les activités suivantes, ce qui synchronise de manière efficace et fiable les LSPDB de tous les IS sur un circuit multiaccès :

- Inonder les LSP qui sont absents de ou sont plus récents que ceux décrits dans les CSNP envoyés par le DIS.
- Demander un LSP en envoyant un PSNP pour les LSP décrits dans les CSNP envoyés par le DIS qui sont absents de la base de données locale ou plus anciens que ce qui est décrit dans l'ensemble CSNP.

Synchronisation LSPDB IS-IS

Le bon fonctionnement d'IS-IS nécessite un processus fiable et efficace pour synchroniser les LSPDB sur chaque IS. Dans IS-IS, ce processus s'appelle le processus de mise à jour. Le processus de mise à jour fonctionne indépendamment à chaque niveau pris en charge. Les LSP générés localement sont toujours de nouveaux LSP. Les LSP reçus d'un voisin sur un circuit peuvent être générés par un autre IS ou être une copie d'un LSP généré par l'IS local. Les LSP reçus peuvent être plus anciens, identiques ou plus récents que le contenu actuel de la LSPDB locale.

Traitement des nouveaux LSP

Lorsqu'un nouveau LSP est ajouté à la LSPDB locale, il remplace une ancienne copie du même LSP dans la LSPDB. Le nouveau LSP est marqué pour être envoyé sur tous les circuits sur lesquels l'IS a actuellement une contiguïté dans l'état UP au niveau associé au nouveau LSP, à l'exception du circuit sur lequel le nouveau LSP a été reçu.

Pour les circuits multiaccès, l'IS inonde une fois le nouveau LSP. L'IS examine l'ensemble des CNSP qui sont envoyés périodiquement par le DIS pour le circuit multiaccès. Si la LSPDB locale contient un ou plusieurs LSP plus récents que ceux décrits dans l'ensemble CSNP (y compris les LSP qui ne figurent pas dans l'ensemble CSNP), ces LSP sont rechargés sur le circuit multiaccès. Si la LSPDB locale contient un ou plusieurs LSP plus anciens que ceux décrits dans l'ensemble CSNP (y compris les LSP décrits dans l'ensemble CSNP qui sont absents de la LSPDB locale), un PSNP est envoyé sur le circuit multiaccès avec les descriptions des LSP qui nécessitent une mise à jour. Le DIS pour le circuit multiaccès répond en envoyant les LSP demandés.

Gestion des anciens LSP

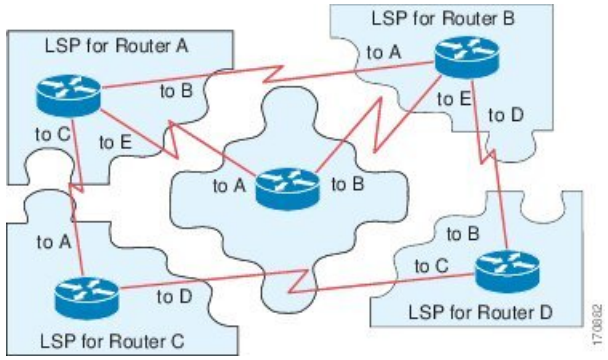
Un IS peut recevoir un LSP plus ancien que la copie dans la LSPDB locale. Un IS peut recevoir un SNP (complet ou partiel) qui décrit un LSP plus ancien que la copie dans la LSPDB locale. Dans les deux cas, l'IS marque le LSP dans la base de données locale à inonder sur le circuit sur lequel le LSP plus ancien ou le SNP contenant le LSP plus ancien a été reçu. Les actions entreprises sont les mêmes que celles décrites ci-dessus après l'ajout d'un nouveau LSP à la base de données locale.

Gestion des LSP du même âge

En raison de la nature distribuée du processus de mise à jour, il est possible qu'un IS reçoive des copies d'un LSP qui sont identiques au contenu actuel de la LSPDB locale. Dans les circuits multiaccès, la réception d'un LSP du même âge est ignorée. La transmission périodique d'un CSNP défini par le DIS pour ce circuit sert de confirmation implicite à l'expéditeur que le LSP a été reçu.

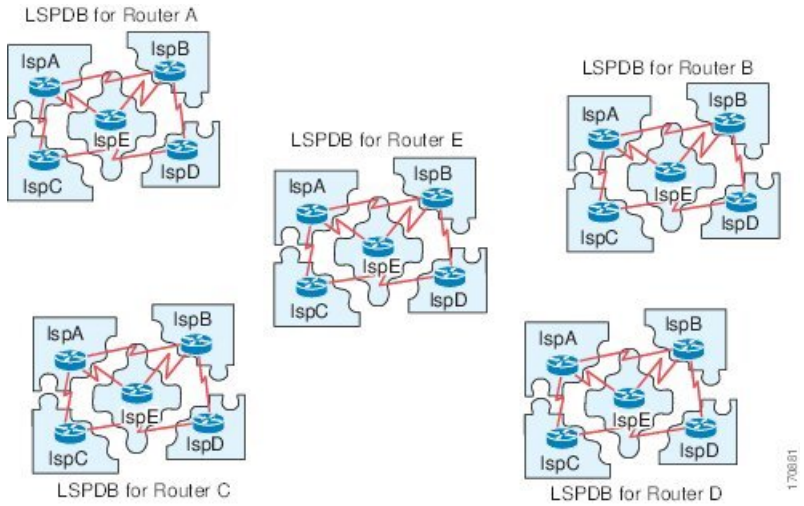
La figure suivante montre comment les LSP sont utilisés pour créer une carte du réseau. Considérez la topologie du réseau comme un casse-tête. Chaque LSP (représentant un IS) est l'une des pièces. Elle s'applique à tous les appareils de niveau 1 dans une zone ou à tous les appareils de niveau 2 dans un sous-domaine de niveau 2.

Illustration 86 : Carte du réseau IS-IS



La figure suivante montre chaque appareil du réseau IS-IS avec sa base de données d'état des liaisons entièrement mise à jour après la formation des contiguïtés entre les appareils voisins. Elle s'applique à tous les appareils de niveau 1 dans une zone ou à tous les appareils de niveau 2 dans un sous-domaine de niveau 2.

Illustration 87 : Périphériques IS-IS avec LSPDB synchronisées



Calcul du chemin le plus court IS-IS

Lorsque le contenu de la LSPDB change, chaque IS exécute indépendamment un calcul du chemin le plus court. L'algorithme est basé sur l'algorithme bien connu de Dijkstra pour trouver les chemins les plus courts le long d'un graphique orienté où les IS sont les sommets du graphe et les liaisons entre les IS sont des arêtes avec un poids non négatif. Une vérification de la connectivité bidirectionnelle est effectuée avant de prendre

en compte une liaison entre deux IS dans le graphique. Cela empêche l'utilisation de renseignements obsolètes dans la LSPDB, par exemple, lorsqu'un IS n'est plus opérationnel dans le réseau, mais n'a pas purgé l'ensemble de LSP qu'il a généré avant d'arrêter son fonctionnement.

La sortie du SPF est un ensemble de tuples (destination, prochain saut). Les destinations sont propres au protocole. Plusieurs chemins à coût égal sont pris en charge, auquel cas plusieurs sauts suivants seront associés à la même destination.

Des SPF indépendants sont effectués pour chaque niveau pris en charge par l'IS. Lorsque la même destination est accessible par les chemins de niveau 1 et 2, le chemin de niveau 1 est privilégié.

Un IS de niveau 2 qui indique qu'il a un ou plusieurs voisins de niveau 2 dans d'autres zones peut être utilisé par des périphériques de niveau 1 dans la même zone que le chemin de dernier recours, également appelé route par défaut. L'IS de niveau 2 indique sa liaison à d'autres zones en définissant un bit de connexion (ATT) dans son LSP de niveau 1 sur 0.

Remarque Un IS peut générer jusqu'à 256 LSP à chaque niveau. Les LSP sont identifiés par les numéros de 0 à 255. Le LSP 0 a des propriétés spéciales, notamment l'importance du réglage du bit ATT pour indiquer l'annexion à d'autres zones. Lorsque les LSP numérotés de 1 à 255 ont le bit ATT activé, ce n'est pas important.

Protocole d'arrêt IS-IS

Vous pouvez fermer IS-IS (le mettre dans un état administratif arrêté) pour apporter des modifications à la configuration du protocole IS-IS sans perdre vos paramètres de configuration. Vous pouvez fermer IS-IS au niveau du processus IS-IS global ou au niveau de l'interface. Si le périphérique a été redémarré lorsque le protocole a été désactivé, celui-ci devrait redémarrer dans un état désactivé. Lorsque le protocole est défini sur l'état administratif désactivé, les administrateurs réseau sont autorisés à désactiver administrativement le fonctionnement du protocole IS-IS sans perdre la configuration du protocole, à apporter une série de modifications à la configuration du protocole sans que le fonctionnement du protocole ne passe par des états intermédiaires, voire indésirables, puis à réactiver le protocole au moment opportun.

Conditions préalables d'IS-IS

Les conditions préalables suivantes sont nécessaires avant de configurer IS-IS :

- Connaissance des protocoles IPv4 et IPv6.
- Vous devez connaître la conception de votre réseau et la façon dont vous souhaitez que le trafic y passe avant de configurer IS-IS.
- Définissez les zones, préparez un plan d'adressage pour les périphériques (y compris la définition des réseaux) et déterminez les interfaces qui exécuteront IS-IS.
- Avant de configurer vos périphériques, préparez une matrice de contiguïtés qui indique les voisins attendus dans le tableau de contiguïté. Cela facilitera la vérification.

Lignes directrices relatives à IS-IS

Directives sur le mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Lignes directrices relatives à la grappe

Pris en charge uniquement en mode d'interface individuelle; le mode EtherChannel étendu n'est pas pris en charge.

Directives supplémentaires

IS-IS n'est pas pris en charge avec le transfert bidirectionnel.

Configurer IS-IS

Cette section décrit comment activer et configurer le processus IS-IS sur votre système.

Procédure

Étape 1 Activer le routage IS-IS globalement, à la page 994.
Étape 2 Activer l'authentification IS-IS, à la page 996.
Étape 3 Configurer LSP IS-IS, à la page 997
Étape 4 Configurer les adresses de résumé IS-IS, à la page 999.
Étape 5 Configurer NET IS-IS, à la page 1000.
Étape 6 Configurer les interfaces passives IS-IS, à la page 1001.
Étape 7 Configurer les interfaces IS-IS, à la page 1002.
Étape 8 Configurer la famille d'adresses IPv4 IS-IS, à la page 1006.
Étape 9 Configurer la famille d'adresses IPv6 IS-IS, à la page 1010.

Activer le routage IS-IS globalement

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List, double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **ISIS** > **General (Général)**.

Étape 2 Cochez la case **Configure ISIS** (Configurer ISIS) pour activer IS-IS.

Étape 3 Cochez la case **Shutdown protocol** (Arrêter le protocole) pour activer le protocole d'arrêt.

Consultez Protocole d'arrêt IS-IS, à la page 993 pour de plus amples renseignements sur le protocole d'arrêt.

Étape 4 Pour que IS-IS utilise un nom d'hôte dynamique, cochez la case **Use dynamic hostname** (Utiliser un nom d'hôte dynamique).

Le nom d'hôte dynamique est activé par défaut. Consultez Nom de domaine dynamique IS-IS, à la page 988 pour obtenir des renseignements détaillés sur le nom d'hôte dynamique dans IS-IS.

Étape 5 Pour empêcher IS-IS de remplir les PDU Hello du réseau local, cochez la case **Do not pad LAN hello PDUs** (Ne pas remplir les PDU Hello du réseau local).

Les Hellos IS-IS sont remplis à la taille de l'unité de transfert maximale (MTU). Cela permet une détection précoce des erreurs résultant de problèmes de transmission avec de grandes trames ou d'erreurs résultant de MTU non concordantes sur des interfaces adjacentes. Vous pouvez désactiver le remplissage Hello pour éviter de gaspiller la bande passante du réseau dans le cas où la MTU des deux interfaces est identique ou en cas de pontage translationnel.

Étape 6 Pour annoncer les interfaces passives uniquement, cochez la case **Advertise passive only** (Annoncer les interfaces passives uniquement).

Elle exclut les préfixes IP des réseaux connectés des annonces LSP, ce qui réduit le temps de convergence IS-IS.

Étape 7 Choisissez si vous souhaitez que votre ASA agisse en tant que routeur de station (niveau 1), en tant que routeur de zone (niveau 2) ou les deux (niveau 1-2) en cliquant sur le bouton radio approprié.

Consultez À propos d'IS-IS, à la page 987 pour en savoir plus sur les niveaux IS-IS.

Étape 8 Dans le champ **Topology priority** (Priorité de la topologie), entrez un numéro qui indique où se trouve la priorité de l'ASA dans la topologie. La valeur doit être comprise entre 0 et 127.

Étape 9 Dans le champ **Route priority tag** (Balise de priorité de route), entrez une balise qui indique la priorité de route de l'ASA. La plage va de 1 à 4294967295. La valeur par défaut est 100. Des valeurs plus élevées indiquent une préférence plus élevée. Cette préférence est envoyée à tous les routeurs du système IS-IS.

Étape 10 Pour que IS annonce expressément qu'il est L2, choisissez un périphérique dans le menu déroulant, puis cliquez sur **Manage** (Gérer).

Consultez Define a Route Map (Définir une carte de routage) pour connaître la procédure d'ajout d'une carte de routage.

Étape 11 Cochez la case **Log changes in adjacency** (Journaliser les modifications de contiguïté) pour que l'ASA envoie un message de journal chaque fois qu'un voisin IS-IS est activé ou désactivé.

Cette commande est désactivée par défaut. La journalisation des modifications de contiguïté est utile lors de la surveillance de grands réseaux.

Étape 12 Pour que les modifications soient incluses à partir d'événements non-IIH, cochez la case **Include changes generated by non-IIH events** (Inclure les modifications générées par les événements non-IIH).

Étape 13 Pour configurer l'intervalle de temps sceptique, saisissez le nombre de minutes dans le champ **Sceptical interval** (Intervalle sceptique). La plage autorisée va de 0 à 1 440 minutes. La valeur par défaut est de cinq minutes.

Étape 14 Cliquez sur **Apply** (Appliquer).

Activer l'authentification IS-IS

L'authentification du routage IS-IS empêche l'introduction de messages de routage non autorisés ou faux provenant de sources non approuvées. Vous pouvez définir un mot de passe pour chaque zone ou domaine IS-IS afin d'éviter que des routeurs non autorisés injectent de faux renseignements de routage dans la base de données sur l'état des liens, ou vous pouvez configurer un type d'authentification IS-IS, soit IS-IS MD5, soit une authentification en texte clair améliorée. Vous pouvez également définir l'authentification par interface. Tous les voisins IS-IS sur les interfaces configurées pour l'authentification des messages IS-IS doivent être configurés avec le même mode d'authentification et la même clé pour que les contiguïtés soient établies.

Consultez À propos d'IS-IS, à la page 987 pour en savoir plus sur les zones et les domaines.

Avant de commencer

Avant de pouvoir activer l'authentification du routage IS-IS, vous devez activer IS-IS et configurer une zone. Reportez-vous à Activer le routage IS-IS globalement, à la page 994 pour connaître la procédure.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **IS-IS** > **Authentication (Authentification)**.

Étape 2 Configurez les paramètres d'authentification pour les niveaux 1 et 2 :

- Dans le champ **Key** (Clé), saisissez la clé pour authentifier les mises à jour IS-IS. La clé peut inclure jusqu'à 16 caractères.
- Cliquez sur le bouton radio **Enable** (Activer) ou **Disable** (Désactiver) selon que vous souhaitez ou non activer l'option Send Only (Envoyer uniquement).

Remarque Les ASA auront plus de temps pour que les clés soient configurées sur chaque ASA si l'authentification est insérée uniquement dans les paquets en cours d'envoi, et n'est pas vérifiée sur les paquets en cours de réception.

- Choisissez le mode d'authentification en cliquant sur le bouton radio **Disabled** (Désactivé), **MD5** ou **Plaintext** (Texte brut).

Étape 3 Si vous choisissez **Disabled** (Désactivé), saisissez un mot de passe de zone pour la zone de niveau 1 (sous-domaine) et/ou un mot de passe de domaine pour le domaine de niveau 2.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer LSP IS-IS

Un IS génère des LSP pour annoncer ses voisins et les destinations qui sont directement connectées à IS-IS. Consultez Types de PDU IS-IS, à la page 988 pour en savoir plus sur les LSP.

Utilisez les commandes suivantes pour configurer les LSP afin d'avoir une configuration de convergence plus rapide.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List, double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **IS-IS** > **Link State Packet (Paquet d'état de liaison)**.

Remarque IS-IS doit être activé avant de pouvoir configurer les paramètres LSP. Reportez-vous à Activer le routage IS-IS globalement, à la page 994 pour connaître la procédure.

Étape 2 Pour permettre à l'ASA d'ignorer les paquets LSP reçus avec des erreurs de somme de contrôle interne plutôt que de purger les LSP, cochez la case **Ignore LSP errors** (Ignorer les erreurs LSP).

Étape 3 Pour inonder rapidement et remplir les LSP avant d'exécuter SPF, cochez la case **Flood LSPs before running SPF** (Inonder les LSP avant d'exécuter SPF), puis dans le champ **Number of LSPs to be flooded** (Nombre de LSP à inonder), entrez un numéro. La plage est comprise entre 1 et 15. La valeur par défaut est égale à 5.

Ce paramètre envoie un nombre spécifié de LSP à partir de l'ASA. Si aucun numéro LSP n'est précisé, la valeur par défaut de 5 est utilisée. Les LSP invoquent SPF avant d'exécuter SPF. Nous vous conseillons d'activer l'inondation rapide, car cela accélère le processus d'inondation des LSP, ce qui améliore le temps de convergence global du réseau.

Étape 4 Pour supprimer les préfixes IP, cochez la case **Suppress IP prefixes** (Supprimer les préfixes IP), puis cochez l'une des options suivantes :

- **Don't advertise IP prefixes learned form another ISIS level when ran out of LSP fragments** (Ne pas annoncer les préfixes IP appris à partir d'un autre niveau ISIS lorsqu'il n'y a plus de fragments LSP) : supprime toutes les routes provenant d'un autre niveau. Par exemple, si le LSP de niveau 2 est complet, les routes du niveau 1 sont supprimées.
- **Don't advertise IP prefixes learned form other protocols when ran out of LSP fragments** (Ne pas annoncer les préfixes IP appris dans d'autres protocoles lorsqu'il n'y a plus de fragments LSP) : supprime toutes les routes redistribuées sur l'ASA.

Dans les réseaux où il n'y a aucune limite au nombre de routes redistribuées dans IS-IS, il est possible que le LSP soit saturé et que les routes soient supprimées. Utilisez ces options pour contrôler les routes qui sont supprimées lorsque la PDU est pleine.

Étape 5 Configurez les intervalles de génération LSP pour les niveaux 1 et 2 :

- **LSP calculation interval** (Intervalle de calcul de LSP) : saisissez l'intervalle de temps en secondes entre la transmission de chaque LSP. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est égale à 5.

  La durée doit être supérieure au délai aller-retour attendu entre deux ASA du réseau connecté. Le nombre doit être prudent, sinon cela entraînera des transmissions inutiles. Les retransmissions se produisent uniquement lorsque les LSP sont abandonnés. Or, le fait de définir une valeur plus élevée pour le nombre a peu d'effet sur la reconvergence. Plus les ASA ont de voisins et plus de chemins sur lesquels les LSP peuvent être inondés, plus vous pouvez augmenter cette valeur.

- **Initial wait for LSP calculation** (Attente initiale pour le calcul du LSP) : saisissez le temps en millisecondes en spécifiant le délai d'attente initial avant la génération du premier LSP. La valeur doit être comprise entre 1 et 120 000. La valeur par défaut est 50.

- **Minimum wait between first and second LSP calculation** (Attente minimum entre le premier et le deuxième calcul du LSP) : saisissez le temps en millisecondes entre la première et la deuxième génération de LSP. La valeur doit être comprise entre 1 et 120 000. La valeur par défaut est 5 000.

Étape 6 Si vous souhaitez que les valeurs que vous avez configurées pour le niveau 1 s'appliquent également au niveau 2, cochez la case **Use level 1 parameters also for level 2** (Utiliser les paramètres du niveau 1 aussi pour le niveau 2).

Étape 7 Dans le champ **Maximum LSP size** (Taille maximale du LSP), saisissez le nombre maximum de secondes entre deux occurrences consécutives de génération d'une LSP. La plage se situe entre 128 et 4352. La valeur par défaut est 1492.

Étape 8 Dans le champ **LSP refresh interval** (Intervalle d'actualisation des LSP), saisissez le nombre de secondes pendant lequel les LSP sont actualisés. La plage est de 1 à 65 535. La valeur par défaut est 900.

L'intervalle d'actualisation détermine la vitesse à laquelle le logiciel transmet périodiquement dans les LSP les renseignements sur la topologie des routes qu'il génère. Il en est ainsi pour éviter que les renseignements de la base de données ne deviennent trop anciens.

La réduction de l'intervalle d'actualisation diminue la durée pendant laquelle une corruption non détectée de la base de données d'état des liaisons peut persister, au détriment d'une utilisation accrue des liaisons. (Cependant, il s'agit d'un événement extrêmement improbable, car il existe d'autres protections contre la corruption.) L'augmentation de l'intervalle réduit l'utilisation de la liaison causée par l'inondation de paquets actualisés (bien que cette utilisation soit très faible).

Étape 9 Dans le champ **Maximum LSP lifetime** (Durée de vie maximale des LSP), saisissez le nombre maximal de secondes pendant lesquelles les LSP peuvent rester dans la base de données d'un routeur sans être actualisés. La plage valide est de 1 à 65535. La valeur par défaut est 1 200 (20 minutes).

Vous devrez peut-être ajuster ce paramètre si vous modifiez l'intervalle d'actualisation du LSP. Les LSP doivent être actualisés périodiquement avant l'expiration de leur durée de vie. La valeur définie pour l'intervalle d'actualisation des LSP doit être inférieure à la valeur définie pour la durée de vie maximale des LSP; sinon, les LSP expireront avant d'être actualisés. Si vous rendez la durée de vie des LSP trop faible par rapport à l'intervalle d'actualisation des LSP, l'intervalle d'actualisation des LSP est automatiquement réduit pour empêcher les LSP d'expirer.

Étape 10 Cliquez sur **Apply** (Appliquer).

Configurer les adresses de résumé IS-IS

Plusieurs groupes d'adresses peuvent être récapitulés pour un niveau donné. Les routes apprises d'autres protocoles de routage peuvent également être résumées. La métrique utilisée pour annoncer le résumé est la plus petite de toutes les routes spécifiques. Cela permet de réduire la taille de la table de routage.

Vous devez définir manuellement les adresses sommaires si vous souhaitez créer des adresses sommaires qui ne se produisent pas à la limite d'un numéro de réseau, ou si vous souhaitez utiliser des adresses sommaires sur l'ASA avec le récapitulatif de routage automatique désactivé.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **IS-IS** > **Summary Address (Adresse sommaire)**.

Le volet **Configure ISIS Summary Address** (Configurer l'adresse sommaire IS-IS) affiche un tableau des adresses sommaires IS-IS définies de manière statique. Par défaut, IS-IS résume les routes de sous-réseau au niveau du réseau. Vous pouvez créer des adresses sommaires IS-IS définies statiquement au niveau du sous-réseau à partir du volet **Configure ISIS Summary Address** (Configurer l'adresse sommaire IS-IS).

Étape 2 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle adresse sommaire IS-IS ou sur **Edit** (Modifier) pour modifier une adresse sommaire IS-IS existante dans le tableau.

La boîte de dialogue **Add Summary Address** (Ajouter une adresse sommaire) ou **Edit Summary Address** (Modifier une adresse sommaire) s'affiche. Vous pouvez également cliquer deux fois sur une entrée du tableau pour la modifier.

Étape 3 Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de la route récapitulative.

Étape 4 Dans le champ **Netmask** (Masque réseau), choisissez ou saisissez le masque réseau à appliquer à l'adresse IP.

Étape 5 Sélectionnez le bouton radio **Level 1** (Niveau 1), **Level 2** (Niveau 2) ou **Level 1 and 2** (Niveau 1 et 2) selon les niveaux auxquels vous souhaitez recevoir des adresses sommaires.

- **Level 1** (Niveau 1) : les routes récapitulatives sont appliquées lors de la redistribution des routes de niveau 1 et niveau 2 et lorsque IS-IS de niveau 2 annonce des routes de niveau 1 comme accessibles dans sa zone.
- **Level 2** (Niveau 2) : les routes apprises par le routage de niveau 1 sont récapitulées dans le réseau fédérateur de niveau 2 avec l'adresse configurée et la valeur de masque. Les routes redistribuées dans IS-IS de niveau 2 sont également résumées.
- **Level 1 and 2** (Niveau 1 et 2) : les routes récapitulatives sont appliquées lors de la redistribution des routes de niveau 1 et niveau 2 et lorsque IS-IS de niveau 2 annonce des routes de niveau 1 comme accessibles dans sa zone.

Étape 6 Dans le champ **Tag** (Balise), saisissez un numéro pour la balise. La plage va de 1 à 4294967295.

Le champ Tag (Balise) vous permet de spécifier un numéro pour baliser les routes qui sont résumées. Si les routes ont déjà été marquées dans le volet **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **ISIS** > **General (Général)** dans le champ **Route priority tag** (Balise de priorité de route), ces routes sont résumées, sinon la balise est perdue.

Étape 7 Dans le champ **Metric** (Mesure), saisissez la mesure qui sera appliquée à la route récapitulative. La plage va de 1 à 4294967295. La valeur par défaut est 10.

La valeur de mesure est attribuée à la liaison et utilisée pour calculer le coût du chemin via les liaisons vers les destinations. Vous pouvez configurer cette mesure pour le routage de niveau 1 ou 2 uniquement.

Étape 8 Cliquez sur **OK**.

Étape 9 Cliquez sur **Apply** (Appliquer).

Configurer NET IS-IS

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List, double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

IS-IS utilise des adresses appelées Network Entity Titres (NET). Elles peuvent avoir une longueur comprise entre 8 et 20 octets, mais ont généralement une longueur de 10 octets. Vous pouvez ajouter une entrée NET sur la page NET lorsque la mise en grappe n'est pas configurée sur l'ASA. Si votre ASA a configuré la mise en grappe, vous devez créer une entrée de groupe réseau dans le volet **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Address Pools (Ensembles d'adresses) > NET Address Pools (Ensembles d'adresses NET)**. Vous pouvez ensuite référencer l'ensemble d'adresses NET dans le volet NET.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **IS-IS** > **Network Entity Title (NET)**.

Le volet **Configure Network Entity (NET)** (Configurer l'entité réseau (NET)) affiche un tableau des adresses NET. Vous pouvez ajouter une entrée NET ici lorsque la mise en grappe n'est PAS configurée sur l'ASA. Pour un ASA avec la mise en grappe configurée, vous devez créer une entrée de groupe réseau dans **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **Address Pools (Ensembles d'adresses)** > **Net Address Pools (Ensembles d'adresses réseau)**.

Vous pouvez ensuite référencer l'ensemble d'adresses NET dans le volet Network Entity Title (NET).

Étape 2 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle adresse NET IS-IS ou sur **Edit** (Modifier) pour modifier une adresse NET IS-IS existante dans le tableau.

La boîte de dialogue **Add Network Entity Title (NET)** (Ajouter Network Entity Title (NET)) ou **Edit Network Entity Title (NET)** (Modifier Network Entity Title (NET)) s'affiche. Vous pouvez également cliquer deux fois sur une entrée du tableau pour la modifier.

Étape 3 Dans la liste déroulante Network Entity Title (NET), choisissez un NET.

Étape 4 Dans le champ **Maximum allowed Net** (NET maximum autorisé), saisissez le nombre maximum de NET autorisés que vous souhaitez. La plage s'étend de 3 à 254. La valeur par défaut est de 3.

Dans la plupart des cas, un seul NET est nécessaire, mais dans le cas de la fusion de plusieurs zones ou de la division d'une zone en plusieurs zones, vous devrez peut-être utiliser plusieurs adresses de zone.

Étape 5 Cliquez sur **Apply** (Appliquer).

Configurer les interfaces passives IS-IS

Vous pouvez désactiver les paquets Hello IS-IS et les mises à jour de routage sur les interfaces tout en incluant les adresses d'interface dans la base de données de topologie. Ces interfaces ne formeront pas de contiguïtés de voisins IS-IS.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage IS-IS, mais qui est associée à un réseau que vous souhaitez annoncer, configurez les interfaces passives pour empêcher cette interface d'utiliser IS-IS. En outre, vous pouvez spécifier la version d'IS-IS utilisée par l'ASA pour les mises à jour. Le routage passif aide à contrôler l'annonce des renseignements de routage IS-IS et désactive l'envoi et la réception des mises à jour de routage IS-IS sur une interface.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **IS-IS** > **Passive Interfaces (Interfaces passives)**.

Étape 2 Pour supprimer les mises à jour de routage sur toutes les interfaces, cochez la case **Suppress routing updates on all Interfaces** (Supprimer les mises à jour de routage sur toutes les interfaces).

Cela fait en sorte que toutes les interfaces fonctionnent en mode passif.

Étape 3 Pour configurer des interfaces individuelles afin de supprimer les mises à jour de routage, sélectionnez l'interface de routage nommée dans la colonne de gauche et cliquez sur **Add** (Ajouter) pour l'ajouter à la colonne Suppress routing updates (Supprimer les mises à jour de routage).

La définition d'un nom d'interface définit uniquement cette interface en mode passif. En mode passif, les mises à jour de routage IS-IS sont acceptées par l'interface spécifiée, mais ne sont pas envoyées à partir de cette interface.

Remarque Seules les interfaces auxquelles vous avez attribué un nom de domaine dynamique peuvent être supprimées de l'envoi de mises à jour de routage. Consultez Nom de domaine dynamique IS-IS, à la page 988 pour de plus amples renseignements.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer les interfaces IS-IS

Cette procédure décrit comment modifier les interfaces ASA individuelles pour le routage IS-IS.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **IS-IS** > **Interface**.

Le volet **IS-IS Interface Configuration** (Configuration de l'interface IS-IS) apparaît et affiche les configurations de l'interface IS-IS. Vous pouvez configurer le remplissage Hello par interface en cochant ou décochant la case **Hello Padding** (Remplissage Hello).

Les Hellos IS-IS sont remplis à la taille de l'unité de transfert maximale (MTU). Le remplissage des hellos IS-IS à la MTU complète permet une détection précoce des erreurs résultant de problèmes de transmission avec de grandes trames ou d'erreurs résultant de MTU non concordantes sur des interfaces adjacentes.

Étape 2 Choisissez une entrée d'interface en double-cliquant sur une entrée d'interface, ou choisissez l'entrée et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit IS-IS Interface** (Modifier l'interface IS-IS) apparaît.

Étape 3 Dans l'onglet **General** (Général), configurez les éléments suivants :

- **Shutdown IS-IS on this interface** (Arrêter IS-IS sur cette interface) : vous permet de désactiver le protocole IS-IS pour cette interface sans supprimer les paramètres de configuration. Le protocole IS-IS ne forme aucune contiguïté sur cette interface et l'adresse IP de cette interface est placée dans le LSP généré par l'ASA.
- **Enable IS-IS on this interface** (Activer IS-IS sur cette interface) : active le protocole IS-IS sur cette interface.
- **Enable IPv6 IS-IS routing on this interface** (Activer le routage IPv6 IS-IS sur cette interface) : active le routage IPv6 IS-IS sur cette interface.
- **Priority for level-1** (Priorité pour le niveau-1) : vous permet de définir une priorité pour le niveau 1. La priorité est utilisée pour déterminer quel routeur d'un réseau local sera le routeur désigné ou le système intermédiaire désigné (DIS). Les priorités sont annoncées dans les paquets Hello. Le routeur ayant la priorité la plus élevée devient le DIS. La valeur doit être comprise entre 0 et 127. La valeur par défaut est 64.



Remarque Dans IS-IS, il n'y a pas de routeur désigné de secours. La définition de la priorité à 0 réduit la probabilité que ce système devienne le DIS, mais ne l'empêche pas. Si un routeur ayant une priorité plus élevée entre en ligne, il prend le rôle du DIS actuel. En cas de priorités égales, l'adresse MAC la plus élevée rompt le lien.

- **Priority for level-2** (Priorité pour le niveau-2) : vous permet de définir une priorité pour le niveau 2. La priorité est utilisée pour déterminer quel routeur d'un réseau local sera le routeur désigné ou le système intermédiaire désigné (DIS). Les priorités sont annoncées dans les paquets Hello. Le routeur ayant la priorité la plus élevée devient le DIS. La valeur doit être comprise entre 0 et 127. La valeur par défaut est 64.

Remarque Dans IS-IS, il n'y a pas de routeur désigné de secours. La définition de la priorité à 0 réduit la probabilité que ce système devienne le DIS, mais ne l'empêche pas. Si un routeur ayant une priorité plus élevée entre en ligne, il prendra le rôle du DIS actuel. En cas de priorités égales, l'adresse MAC la plus élevée rompt le lien.

- **Tag** (Balise) : définit une balise sur l'adresse IP configurée pour une interface lorsque ce préfixe IP est placé dans un LSP IS-IS.
- **CSNP Interval for level-1** (Intervalle CSNP pour le niveau-1) : définit l'intervalle des PDU du numéro de séquence complet (CSNP) en secondes entre la transmission des CSNP sur les réseaux multiaccès pour le niveau 1. Cet intervalle s'applique uniquement à l'ASA désigné. La valeur doit être comprise entre 0 et 65 535. La valeur par défaut est de 10 secondes. Il est peu probable que vous deviez modifier la valeur par défaut.

  Cette option s'applique uniquement au routeur désigné (DR) pour une interface donnée. Seuls les DR envoient des paquets CSNP pour maintenir la synchronisation de la base de données.

- **CSNP Interval for level-2** (Intervalle CSNP pour le niveau-2) : définit l'intervalle des PDU du numéro de séquence complet (CSNP) en secondes entre la transmission des CSNP sur les réseaux multiaccès pour le niveau 2. Cet intervalle s'applique uniquement à l'ASA désigné. La valeur doit être comprise entre 0 et 65 535. La valeur par défaut est de 10 secondes. Il est peu probable que vous deviez modifier la valeur par défaut.

  Cette option s'applique uniquement au routeur désigné (DR) pour une interface donnée. Seuls les DR envoient des paquets CSNP pour maintenir la synchronisation de la base de données.

- **Adjacency filter** (Filtre de contiguïté) : filtre l'établissement des contiguïtés IS-IS.

  Le filtrage est effectué en créant des adresses NSAP à partir des paquets Hello IS-IS entrants en combinant chaque adresse de zone du Hello avec l'ID de système. Chacune de ces adresses NSAP est ensuite transmise par le filtre. Si un NSAP correspond, le filtre est considéré comme transmis, sauf si vous avez spécifié **Match all area addresses** (Faire correspondre toutes les adresses de zone), auquel cas toutes les adresses doivent passer. La fonctionnalité de **Match all area addresses** (Faire correspondre toutes les adresses de zone) est utile pour effectuer des tests négatifs, comme l'acceptation d'une contiguïté uniquement si une adresse particulière n'est PAS présente.

- **Match all area addresses** (Faire correspondre toutes les adresses de zone) : (Facultatif) toutes les adresses NSAP doivent correspondre au filtre pour accepter la contiguïté. Si elle n'est pas spécifiée (par défaut), une seule adresse doit correspondre au filtre pour que la contiguïté soit acceptée.

Étape 4 Cliquez sur **OK**.

Étape 5 Sous l'onglet **Authentication** (Authentification), configurez les éléments suivants pour le niveau 1 et/ou le niveau 2 :

- Dans le champ **Key** (Clé), saisissez la clé pour authentifier les mises à jour IS-IS. La valeur est comprise entre 0 et 8 caractères.

  Si aucun mot de passe n'est configuré avec l'option **Key** (Clé), aucune authentification par clé n'est effectuée.

- Pour **Send only** (Envoyer uniquement), cliquez sur le bouton radio **Enable** (Activer) ou **Disable** (Désactiver).

Choisir **Send only** (Envoyer uniquement) permet au système d'insérer uniquement le mot de passe dans les SNP, mais de ne pas vérifier le mot de passe dans les SNP qu'il reçoit. Utilisez ce mot clé lors d'une mise à niveau logicielle pour faciliter la transition. Ce paramètre est désactivé par défaut.

- Choisissez le mode d'authentification en cochant la case **Mode**, puis choisissez **MD5** ou **Text** (Texte) dans la liste déroulante, et dans le champ **Password** (Mot de passe), saisissez un mot de passe.

Étape 6 Cliquez sur **OK**.

Étape 7 Dans l'onglet **Hello Padding** (Remplissage Hello), configurez les éléments suivants :

- **Hello Padding** (Remplissage Hello) : active le remplissage Hello.

  Les Hellos IS-IS sont remplis à la taille de l'unité de transfert maximale (MTU). Le remplissage des hellos IS-IS à la MTU complète permet une détection précoce des erreurs résultant de problèmes de transmission avec de grandes trames ou d'erreurs résultant de MTU non concordantes sur des interfaces adjacentes.

- **Minimal holdtime 1 second for Level-1** (Délai de rétention minimum de 1 seconde pour le niveau-1) : active le délai de rétention (en secondes) pendant lequel le LSP reste valide pour le niveau 1.

- **Hello Interval for level-1** (Intervalle Hello pour le niveau-1) : spécifie la durée en secondes entre les paquets Hello pour le niveau 1.

  Par défaut, une valeur de trois fois les secondes d'intervalle Hello est annoncée comme délai de rétention dans les paquets Hello envoyés. (Modifiez le multiplicateur de 3 en cochant la case **Hello Multiplier** (Multiplicateur Hello).) Avec des intervalles Hello plus petits, les modifications topologiques sont détectées plus rapidement, mais le trafic de routage est plus élevé. La plage valide est de 1 à 65 535. La valeur par défaut est 10.

- **Minimal holdtime 1 second for Level-2** (Délai de rétention minimum de 1 seconde pour le niveau-2) : active le délai de rétention (en secondes) pendant lequel le LSP reste valide pour le niveau 2.

- **Hello Interval for level-2** (Intervalle Hello pour le niveau-2) : spécifie la durée en secondes entre les paquets Hello pour le niveau 2.

  Par défaut, une valeur de trois fois les secondes d'intervalle Hello est annoncée comme délai de rétention dans les paquets Hello envoyés. (Modifiez le multiplicateur de 3 en cochant la case **Hello Multiplier** (Multiplicateur Hello).) Avec des intervalles Hello plus petits, les modifications topologiques sont détectées plus rapidement, mais le trafic de routage est plus élevé. La plage valide est de 1 à 65 535. La valeur par défaut est 10.

- **Hello Multiplier for level-1** (Multiplicateur Hello pour le niveau-1) : spécifie le nombre de paquets Hello IS-IS qu'un voisin doit rater avant que l'ASA déclare que la contiguïté est inactive pour le niveau 1.

  Le délai de rétention annoncé dans les paquets hello IS-IS est défini comme le produit du multiplicateur hello par l'intervalle hello. Les voisins déclarent une contiguïté à cet ASA après n'avoir reçu aucun paquet Hello IS-IS pendant le délai de rétention annoncé. Le délai de rétention (et donc le multiplicateur Hello et l'intervalle Hello) peut être défini par interface et peut être différent entre différents ASA dans une zone. La valeur doit être comprise entre 3 et 1 000. La valeur par défaut est de 3.

- **Hello Multiplier for level-2** (Multiplicateur Hello pour le niveau-2) : spécifie le nombre de paquets Hello IS-IS qu'un voisin doit rater avant que l'ASA déclare que la contiguïté est inactive pour le niveau 2.

  Le délai de rétention annoncé dans les paquets hello IS-IS est défini comme le produit du multiplicateur hello par l'intervalle hello. Les voisins déclarent une contiguïté à cet ASA après n'avoir reçu aucun paquet Hello IS-IS pendant le délai de rétention annoncé. Le délai de rétention (et donc le multiplicateur

Hello et l'intervalle Hello) peut être défini par interface et peut être différent entre différents ASA dans une zone. La valeur doit être comprise entre 3 et 1 000. La valeur par défaut est de 3.

- **Configure Circuit Type** (Configurer le type de circuit) : spécifie si l'interface est configurée pour le routage local (niveau 1), le routage de zone (niveau 2) ou le routage local et de zone (niveau 1-2).

Étape 8 Cliquez sur **OK**.

Étape 9 Sous l'onglet **LSP Settings** (Paramètres LSP), configurez les éléments suivants :

- **Advertise IS-IS Prefix** (Annoncer le préfixe IS-IS) : permet l'annonce des préfixes IP des réseaux connectés dans les annonces LSP par interface IS-IS.

  La désactivation de cette option est un mécanisme IS-IS pour exclure le préfixe IP du réseau connecté des annonces LSP, réduisant ainsi le temps de convergence IS-IS.

- **Retransmit Interval** (Intervalle de retransmission) : spécifie le temps en secondes entre la retransmission de chaque LSP IS-IS.

  La durée doit être supérieure au délai aller-retour attendu entre deux ASA du réseau connecté. La valeur est comprise entre 0 et 65 535. La valeur par défaut est égale à 5.

- **Retransmit Throttle Interval (Intervalle de limitation de retransmission)** : spécifie le temps en millisecondes entre les retransmissions sur chaque LSP IS-IS.

  Cette option peut être utile dans de très grands réseaux avec de nombreux LSP et de nombreuses interfaces comme moyen de contrôler le trafic de retransmission des LSP. Cette option contrôle le débit auquel les LSP peuvent être renvoyés sur l'interface. La valeur est comprise entre 0 et 65 535. La valeur par défaut est 33.

- **LSP Interval** (Intervalle LSP) : précise le délai en millisecondes entre les transmissions successives de LSP IS-IS.

  Dans les topologies avec un grand nombre de voisins et d'interfaces IS-IS, un ASA peut avoir de la difficulté avec la charge de CPU imposée par la transmission et la réception des LSP. Cette option permet de réduire le débit de transmission des LSP (et, par conséquent, le débit de réception des autres systèmes). La plage va de 1 à 4294967295. La valeur par défaut est 33.

Étape 10 Cliquez sur **OK**.

Étape 11 Sous l'onglet **Metrics** (Mesures), configurez les options suivantes pour les niveaux 1 et 2 :

Vous pouvez cocher la case **Use the level 1 values also for level 2** (Utiliser les valeurs du niveau 1 aussi pour le niveau 2) si vous souhaitez les mêmes mesures pour les deux niveaux.

- **Use maximum metric value** (Utiliser la valeur de mesure maximum) : spécifie la mesure attribuée au lien et utilisée pour calculer le coût de chaque autre routeur par les liaisons du réseau vers d'autres destinations.

- **Default metric** (Mesure par défaut) : saisissez le numéro de la mesure.

  La valeur est comprise entre 1 et 16777214. La valeur par défaut est 10.

Étape 12 Cliquez sur **OK**.

Étape 13 Cliquez sur **Apply** (Appliquer).

Configurer la famille d'adresses IPv4 IS-IS

Les routeurs sont autorisés à redistribuer des préfixes externes ou des routes apprises à partir de tout autre protocole de routage, configuration statique ou interface connectée. Les routes redistribuées sont autorisées dans un routeur de niveau 1 ou dans un routeur de niveau 2.

Vous pouvez configurer la contiguïté, Shortest Path First (SPF) et vous pouvez définir les conditions pour la redistribution des routes à partir d'un autre domaine de routage dans IS-IS (redistribution) pour les adresses IPv4.

Avant de commencer

Avant de pouvoir activer l'authentification du routage IS-IS, vous devez activer IS-IS et configurer une zone. Reportez-vous à Activer le routage IS-IS globalement, à la page 994 pour connaître la procédure.

Assurez-vous qu'IPv4 est activé sur au moins une interface avant d'essayer d'ajouter un voisin, ou ASDM renvoie un message d'erreur indiquant que la configuration a échoué.

Procédure

Étape 1 Choisissez **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > ISIS > IPv4 Address Family (Famille d'adresses IPv4) > General (Général)**.

a) Cochez la case **Perform adjacency check** (Effectuer une vérification de la contiguïté) pour que le routeur vérifie les routeurs IS à proximité.

b) Dans le champ **Administrative Distance** (Distance administrative), saisissez une distance attribuée aux routes détectées par le protocole IS-IS.

La distance administrative est un paramètre utilisé pour comparer les routes entre différents protocoles de routage. En général, plus la valeur est élevée, plus le taux de confiance est bas. De plus, une distance administrative de 255 signifie que la source de renseignements de routage n'est pas du tout fiable et doit être ignorée. La plage va de 1 à 255. La valeur par défaut est 1.

Vous pouvez utiliser l'option de distance pour configurer les distances administratives appliquées aux routes IS-IS lorsqu'elles sont insérées dans la base de renseignements de routage (RIB) et influer sur la probabilité que ces routes soient préférées aux routes vers les mêmes adresses de destination découvertes par d'autres protocoles.

c) Dans le champ **Maximum number of forward paths** (Nombre maximum de chemins de renvoi), saisissez le nombre maximum de routes IS qui peuvent être installées dans une table de routage. La plage va de 1 à 8.

d) Cochez la case **Distribute default route** (Distribuer la route par défaut) pour configurer un processus de routage IS afin de distribuer une route par défaut, puis choisissez la route par défaut dans la liste déroulante ou cliquez sur **Manage** (Gérer) pour créer une nouvelle route. Consultez Définir une carte de routage, à la page 885 pour connaître la procédure de création d'une nouvelle route.

Étape 2 Configurez les mesures IS-IS :

a) Dans le champ **Global ISIS metric for level 1** (Mesure IS-IS globale pour le niveau 1), saisissez un nombre qui spécifie la mesure.

La plage est de 1 à 63. La valeur par défaut est 10.

Lorsque vous devez modifier la valeur de mesure par défaut pour toutes les interfaces IS-IS , nous vous recommandons d'utiliser l'option **de mesure globale ISIS pour le niveau 1** afin de configurer toutes les

interfaces à l'échelle mondiale. La configuration globale des valeurs de mesure évite les erreurs d'utilisateur, telles que la suppression involontaire d'une mesure définie d'une interface sans configuration de nouvelle valeur et la possibilité involontaire que l'interface reviendra à la mesure par défaut de 10, devenant ainsi une interface de prédilection dans le réseau.

b) Dans le champ **Global ISIS metric for level 2** (Mesure IS-IS globale pour le niveau 2), saisissez un nombre qui spécifie la mesure.

La plage est de 1 à 63. La valeur par défaut est 10.

Lorsque vous devez modifier la valeur de mesure par défaut pour toutes les interfaces IS-IS , nous vous recommandons d'utiliser l'option **de mesure globale ISIS pour le niveau 1** afin de configurer toutes les interfaces à l'échelle mondiale. La configuration globale des valeurs de mesure évite les erreurs d'utilisateur, telles que la suppression involontaire d'une mesure définie d'une interface sans configuration de nouvelle valeur et la possibilité involontaire que l'interface reviendra à la mesure par défaut de 10, devenant ainsi une interface de prédilection dans le réseau.

c) Choisissez l'une des options suivantes pour configurer le type, la longueur et les valeurs (TLV) :

- Cochez la case **Send and accept both styles of TLVs during transition** (Envoyer et accepter les deux styles de TLV pendant la transition).
- Cliquez sur le bouton radio **Use old style of TLVs with narrow metric** (Utiliser l'ancien style de TLV avec mesure restreinte).
- Cliquez sur le bouton radio **Use new style TLVs to carry wider metric** (Utiliser le nouveau style de TLV pour transporter une mesure plus large).

  Si vous choisissez l'un des boutons radio, vous pouvez également cocher la case **Accept both styles of TLVs during transition** (Accepter les deux styles de TLV pendant la transition).

  Nous vous conseillons fortement d'utiliser le nouveau type de TLV, car les TLV utilisés pour annoncer les renseignements IPv4 dans les LSP sont définis pour utiliser uniquement des mesures étendues. Le logiciel prend en charge un champ de mesure de 24 bits, la mesure large. Avec le nouveau style de mesure, les mesures de lien ont désormais une valeur maximale de 16777214 avec une mesure de chemin totale de 4261412864.

d) Cochez la case **Apply metric type to** (Appliquer le type de mesure à), puis cochez la case **Level-1** (Niveau 1) et/ou **Level-2** (Niveau 2).

Étape 3 Cliquez sur **Apply** (Appliquer).

Étape 4 Choisissez **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > ISIS > IPv4 Address Family (Famille d'adresses IPv4) > SPF**.

a) Cochez la case **Honour external metrics during SPF calculations** (Respecter les mesures externes pendant les calculs SPF), pour que les calculs SPF incluent des mesures externes.

b) Cochez la case **Signal other routers not to use this router as an intermediate hop in their SPF calculations** (Signaler aux autres routeurs de ne pas utiliser ce routeur comme saut intermédiaire dans leurs calculs SPF) si vous souhaitez exclure ce périphérique et configurer les éléments suivants :

- Cochez la case **Specify on-startup behavior** (Spécifier le comportement au démarrage) et choisissez l'une des options suivantes :
  - **Advertise ourself as overloaded until BGP has converged** (Se signaler comme surchargé jusqu'à ce que le BGP ait convergé)

- **Specify time to advertise ourself as overloaded after reboot** (Spécifier le délai pour se signaler comme surchargé après le redémarrage)

  Dans le champ **Time to advertise ourself as overloaded** (Délai pour se signaler comme surchargé), saisissez les secondes d'attente jusqu'à ce que le routeur annonce qu'il est surchargé. La plage va de 5 à 86 400 secondes.

- Cochez la case **Don't advertise IP prefixes learned from other protocols when overload bit it set** (Ne pas annoncer les préfixes IP appris à partir d'autres protocoles lorsque le bit de surcharge est défini) pour exclure les préfixes IP.
- Cochez la case **Don't advertise IP prefixes learned from another ISIS level when overload bit is set** (Ne pas annoncer les préfixes IP appris à partir d'un autre niveau ISIS lorsque le bit de surcharge est défini) pour exclure les préfixes IP.

c) Configurez les intervalles de calcul de routage partiel (PRC) :

- Dans le champ **PRC Interval** (Intervalle PRC), saisissez une durée d'attente du routeur entre les calculs de routage partiel (PRC). La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 5 secondes.
- Dans le champ **Initial wait for PRC** (Attente initiale pour le PRC), saisissez le délai initial de calcul du PRC (en millisecondes) après une modification de la topologie. La plage va de 100 à 120 000 millisecondes. La valeur par défaut est de 2 000 millisecondes.
- Dans le champ **Minimum wait between first and second PRC** (Délai d'attente minimum entre le premier et le deuxième PRC), saisissez la durée en millisecondes pendant laquelle vous souhaitez que le routeur attende entre les PRC. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 000 millisecondes.

d) Configurez les intervalles pour les calculs SPF pour les niveaux 1 et 2 :

Remarque Cochez la case **Use level 1 values also for level 2** (Utiliser les valeurs du niveau 1 également pour le niveau 2) si vous souhaitez que les deux niveaux aient les mêmes valeurs.

- Dans le champ **SPF Calculation Interval** (Intervalle de calcul SPF), saisissez un délai d'attente du routeur entre les calculs SPF. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 10 secondes.
- Dans le champ **Initial wait for SPF calculation** (Attente initiale pour le calcul SPF), saisissez le délai d'attente du routeur pour un calcul SPF. La plage va de 100 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes.
- Dans le champ **Minimum wait between first and second SPF calculation** (Délai d'attente minimum entre le premier et le deuxième calcul SPF), saisissez la durée en millisecondes pendant laquelle vous souhaitez que le routeur attende entre les calculs SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes.

Étape 5 Cliquez sur **Apply** (Appliquer).

Étape 6 Choisissez **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > ISIS > IPv6 Address Family (Famille d'adresses IPv6) > Redistribution**.

Le volet **Redistribution** affiche un tableau des routes de redistribution.

Étape 7 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle route de redistribution, ou cliquez sur **Edit** (Modifier) pour modifier une route de redistribution dans le tableau.

La boîte de dialogue **Add Redistribution** (Ajouter une redistribution) ou **Edit Redistribution** (Modifier la redistribution) s'affiche. Vous pouvez également cliquer deux fois sur une entrée du tableau pour la modifier.

a) Dans la liste déroulante **Source Protocol** (Protocole source), choisissez le protocole (BGP, connecté, EIGRP, OSPF, RIP ou statique) à partir duquel vous souhaitez redistribuer les routes dans le domaine ISIS.
b) Dans la liste déroulante **Process ID** (ID de processus), choisissez un ID de processus pour le protocole source.
c) Dans la liste déroulante **Route Level** (Niveau de routage), choisissez le niveau 1, le niveau 2 ou le niveau 1-2.
d) (Facultatif) Dans le champ **Metric** (Mesure), saisissez une mesure pour la route redistribuée. La plage va de 1 à 4294967295.
e) Pour le **Metric Type** (Type de mesure), cliquez sur le bouton radio interne ou externe.
f) Dans la liste déroulante **Route Map** (Carte de routage), choisissez une carte de routage qui doit être inspectée pour filtrer les réseaux à redistribuer, ou cliquez sur **Manage** (Gérer) pour ajouter une nouvelle carte de routage ou modifier une carte de routage existante. Reportez-vous à la section Définir une carte de routage pour connaître la procédure de configuration des cartes de routage.
g) Cochez une ou plusieurs des cases **Match** (Correspondance) (interne, externe 1, externe 2, NSSA externe 1 et NSSA externe 2) pour redistribuer les routes à partir d'un réseau OSPF.

   Cette étape s'applique uniquement à la redistribution à partir des réseaux OSPF.

Étape 8 Cliquez sur **OK**.

Étape 9 Cliquez sur **Apply** (Appliquer).

Configuration du bit associé

Dans l'exemple suivant, le bit associé restera défini lorsque le routeur correspondra à 49.00aa dans la table de routage L2 CLNS :

```
ciscoasa(config)# router isis
 ciscoasa(config-router)# clns filter-set L2_backbone_connectivity permit 49.00aa
 ciscoasa(config-router)# route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# match clns address L2_backbone_connectivity
ciscoasa(config)# router isis
 ciscoasa(config-router)#set-attached-bit route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# end
 ciscoasa# show clns route 49.00aa

Known via "isis", distance 110, metric 30, Dynamic Entry
Routing Descriptor Blocks:
 via tr2, Serial0
   isis, route metric is 30, route version is 58
```

Configurer la famille d'adresses IPv6 IS-IS

Vous pouvez configurer la contiguïté, SPF et vous pouvez définir les conditions pour la redistribution des routes à partir d'un autre domaine de routage dans IS-IS (redistribution) pour les adresses IPv6.

Avant de commencer

Avant de pouvoir activer l'authentification du routage IS-IS, vous devez activer IS-IS et configurer une zone. Reportez-vous à Activer le routage IS-IS globalement, à la page 994 pour connaître la procédure.

Assurez-vous qu'IPv6 est activé sur au moins une interface avant d'essayer d'ajouter un voisin, ou ASDM renvoie un message d'erreur indiquant que la configuration a échoué.

Procédure

Étape 1 Choisissez **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > ISIS > IPv6 Address Family (Famille d'adresses IPv6) > General (Général)**.

a) Cochez la case **Perform adjacency check** (Effectuer une vérification de la contiguïté) pour que le routeur vérifie les routeurs IS à proximité.

b) Dans le champ **Administrative Distance** (Distance administrative), entrez une distance pour la route. La plage va de 1 à 255. La valeur par défaut est 1.

La distance administrative est un paramètre utilisé pour comparer les routes entre différents protocoles de routage. En général, plus la valeur est élevée, plus le taux de confiance est bas. De plus, une distance administrative de 255 signifie que la source de renseignements de routage n'est pas du tout fiable et doit être ignorée. La plage va de 1 à 255. La valeur par défaut est 1.

Vous pouvez utiliser l'option de distance pour configurer les distances administratives appliquées aux routes IS-IS lorsqu'elles sont insérées dans la base de renseignements de routage (RIB) et influer sur la probabilité que ces routes soient préférées aux routes vers les mêmes adresses de destination découvertes par d'autres protocoles.

c) Dans le champ **Maximum number of forward paths** (Nombre maximum de chemins de renvoi), saisissez le nombre maximum de routes IS qui peuvent être installées dans une table de routage. La plage va de 1 à 8.

d) Cochez la case **Distribute default route** (Distribuer la route par défaut) pour configurer un processus de routage IS afin de distribuer une route par défaut, puis choisissez la route par défaut dans la liste déroulante ou cliquez sur **Manage** (Gérer) pour créer une nouvelle route. Consultez Définir une carte de routage, à la page 885 pour connaître la procédure de création d'une nouvelle route.

Étape 2 Cliquez sur **Apply** (Appliquer).

Étape 3 Choisissez **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > ISIS > IPv6 Address Family (Famille d'adresses IPv6) > SPF**.

a) Cochez la case **Signal other routers not to use this router as an intermediate hop in their SPF calculations** (Signaler aux autres routeurs de ne pas utiliser ce routeur comme saut intermédiaire dans leurs calculs SPF) si vous souhaitez exclure ce périphérique et configurer les éléments suivants :

- Cochez la case **Specify on-startup behavior** (Spécifier le comportement au démarrage) et choisissez l'une des options suivantes :
  - **Advertise ourself as overloaded until BGP has converged** (Se signaler comme surchargé jusqu'à ce que le BGP ait convergé)

- **Specify time to advertise ourself as overloaded after reboot** (Spécifier le délai pour se signaler comme surchargé après le redémarrage)

  Dans le champ **Time to advertise ourself as overloaded** (Délai pour se signaler comme surchargé), saisissez les secondes d'attente jusqu'à ce que le routeur annonce qu'il est surchargé. La plage va de 5 à 86 400 secondes.

- Cochez la case **Don't advertise IP prefixes learned from other protocols when overload bit it set** (Ne pas annoncer les préfixes IP appris à partir d'autres protocoles lorsque le bit de surcharge est défini) pour exclure les préfixes IP.
- Cochez la case **Don't advertise IP prefixes learned from another ISIS level when overload bit is set** (Ne pas annoncer les préfixes IP appris à partir d'un autre niveau ISIS lorsque le bit de surcharge est défini) pour exclure les préfixes IP.

b) Configurez les intervalles de calcul de routage partiel (PRC) :

- Dans le champ **PRC Interval** (Intervalle PRC), saisissez une durée d'attente du routeur entre les calculs de routage partiel (PRC). La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 5 secondes.
- Dans le champ **Initial wait for PRC** (Attente initiale pour le PRC), saisissez le délai d'attente du routeur pour un PRC. La plage va de 100 à 120 000 millisecondes. La valeur par défaut est de 2 000 millisecondes.
- Dans le champ **Minimum wait between first and second PRC** (Délai d'attente minimum entre le premier et le deuxième PRC), saisissez la durée en millisecondes pendant laquelle vous souhaitez que le routeur attende entre les PRC. La plage va de 100 à 120 000 millisecondes. La valeur par défaut est de 5 000 millisecondes.

c) Configurez les intervalles pour les calculs SPF pour les niveaux 1 et 2 :



Remarque Cochez la case **Use level 1 values also for level 2** (Utiliser les valeurs du niveau 1 également pour le niveau 2) si vous souhaitez que les deux niveaux aient les mêmes valeurs.

- Dans le champ **SPF Calculation Interval** (Intervalle de calcul SPF), saisissez un délai d'attente du routeur entre les calculs SPF. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 10 secondes.
- Dans le champ **Initial wait for SPF calculation** (Attente initiale pour le calcul SPF), saisissez le délai d'attente du routeur pour un calcul SPF. La plage va de 100 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes.
- Dans le champ **Minimum wait between first and second SPF calculation** (Délai d'attente minimum entre le premier et le deuxième calcul SPF), saisissez la durée en millisecondes pendant laquelle vous souhaitez que le routeur attende entre les calculs SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes.

Étape 4 Cliquez sur **Apply** (Appliquer).

Étape 5 Choisissez **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > ISIS > IPv6 Address Family (Famille d'adresses IPv6) > Redistribution**.

Le volet **Redistribution** affiche un tableau des routes de redistribution.

Étape 6 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle route de redistribution, ou cliquez sur **Edit** (Modifier) pour modifier une route de redistribution dans le tableau.

La boîte de dialogue **Add Redistribution** (Ajouter une redistribution) ou **Edit Redistribution** (Modifier la redistribution) s'affiche. Vous pouvez également cliquer deux fois sur une entrée du tableau pour la modifier.

a) Dans la liste déroulante **Source Protocol** (Protocole source), choisissez le protocole (BGP, connecté, EIGRP, OSPF, RIP ou statique) à partir duquel vous souhaitez redistribuer les routes dans le domaine ISIS.
b) Dans la liste déroulante **Process ID** (ID de processus), choisissez un ID de processus pour le protocole source.
c) Dans la liste déroulante **Route Level** (Niveau de routage), choisissez le niveau 1, le niveau 2 ou le niveau 1-2.
d) (Facultatif) Dans le champ **Metric** (Mesure), saisissez une mesure pour la route redistribuée. La plage va de 1 à 4294967295.
e) Pour le **Metric Type** (Type de mesure), cliquez sur le bouton radio **internal** (interne) ou **external** (externe) pour spécifier le type de mesure pour le protocole de routage de destination.
f) Dans la liste déroulante **Route Map** (Carte de routage), choisissez une carte de routage qui doit être inspectée pour filtrer les réseaux à redistribuer, ou cliquez sur **Manage** (Gérer) pour ajouter une nouvelle carte de routage ou modifier une carte de routage existante. Reportez-vous à la section Définir une carte de routage pour connaître la procédure de configuration des cartes de routage.
g) Cochez une ou plusieurs des cases **Match** (Correspondance) (interne, externe 1, externe 2, NSSA externe 1 et NSSA externe 2) pour redistribuer les routes à partir d'un réseau OSPF.

   Cette étape s'applique uniquement à la redistribution à partir des réseaux OSPF.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Supervision IS-IS

Vous pouvez utiliser les écrans suivants pour superviser le processus de routage IS-IS.

- **Monitoring (Supervision) > Routing (Routage) > ISIS Neighbors (Voisins ISIS)** Ce volet affiche des renseignements sur chaque voisin IS-IS.

  Chaque ligne représente un voisin IS-IS. Pour chaque voisin, la liste comprend l'ID système, le type, l'interface, l'adresse IP, l'état (actif, inactif, etc.), le délai de rétention et l'ID de circuit.

- **Monitoring (Supervision) > Routing (Routage) > ISIS RIB (RIB IS-IS)** Ce volet affiche le tableau local de renseignements de routage IS-IS (RIB).

- **Monitoring (Supervision) > Routing (Routage) > ISIS IPv6 RIB (RIB IPv6 IS-IS)** Ce volet affiche le tableau de renseignements de routage IPv6 IS-IS local.

Historique d'IS-IS

Tableau 43 : Historique des fonctionnalités pour IS-IS

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage IS-IS	9.6(1)	L'ASA prend désormais en charge le protocole de routage IS-IS (Intermediate System to Intermediate System). Une prise en charge a été ajoutée pour le routage des données, l'exécution de l'authentification, ainsi que la redistribution et la supervision des informations de routage à l'aide du protocole de routage IS-IS. Nous avons introduit les écrans suivants : **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > IS-IS** **Monitoring (Supervision) > Routing (Routage) > IS-IS**



CHAPITRE 36

EIGRP

Ce chapitre décrit comment configurer l'ASA pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole Enhanced Interior Gateway Routing Protocol (EIGRP).

- À propos d'EIGRP, à la page 1015
- Lignes directrices relatives à l'EIGRP, à la page 1017
- Configurer un processus EIGRP, à la page 1018
- Configurer le protocole EIGRP, à la page 1018
- Personnaliser l'EIGRP, à la page 1021
- Supervision de l'EIGRP, à la page 1035
- Historique d'EIGRP, à la page 1036

À propos d'EIGRP

L'EIGRP est une version améliorée du protocole IGRP développée par Cisco. Contrairement à IGRP et RIP, EIGRP n'envoie pas de mises à jour périodiques de routage. Les mises à jour du protocole EIGRP sont envoyées uniquement lorsque la topologie du réseau change. Les principales fonctionnalités qui distinguent le protocole EIGRP des autres protocoles de routage comprennent la convergence rapide, la prise en charge des masques de sous-réseau de longueur variable, des mises à jour partielles et de plusieurs protocoles de couche réseau.

Un routeur exécutant EIGRP stocke toutes les tables de routage des voisins afin qu'il puisse s'adapter rapidement aux autres routes. Si aucune route appropriée n'existe, le protocole EIGRP interroge ses voisins pour découvrir une autre route. Ces requêtes se propagent jusqu'à ce qu'une autre route soit trouvée. Sa prise en charge pour les filtres d'adresse locale de longueur variable permet aux routes d'être récapitulées automatiquement sur une limite du nombre de réseaux. De plus, l'EIGRP peut être configuré pour résumer n'importe quelle limite de bits à n'importe quelle interface. Le protocole EIGRP ne fait pas de mises à jour périodiques. Au lieu de cela, il envoie des mises à jour partielles uniquement lorsque la mesure d'une route change. La propagation des mises à jour partielles est automatiquement limitée de sorte que seuls les routeurs qui ont besoin des renseignements sont mis à jour. En raison de ces deux fonctionnalités, EIGRP consomme beaucoup moins de bande passante qu'IGRP.

La découverte de voisin est le processus utilisé par l'ASA pour se familiariser dynamiquement avec la présence d'autres routeurs sur les réseaux directement connectés. Les routeurs EIGRP envoient des paquets Hello en multidiffusion pour annoncer leur présence sur le réseau. Lorsque l'ASA reçoit un paquet Hello d'un nouveau voisin, il envoie son tableau de topologie au voisin avec un bit d'initialisation activé. Lorsque le voisin reçoit la mise à jour de la topologie avec le bit d'initialisation activé, le voisin renvoie sa table de topologie à l'ASA.

Les paquets Hello sont envoyés en tant que messages en multidiffusion. Un message Hello n'attend aucune réponse. L'exception à cette règle concerne les voisins définis de manière statique. Si vous utilisez la commande **neighbor** ou configurez l'intervalle Hello dans ASDM pour configurer un voisin, les messages Hello envoyés à ce voisin sont envoyés en tant que messages de monodiffusion. Les mises à jour de routage et les accusés de réception sont envoyés en tant que messages de monodiffusion.

Une fois cette relation de voisin établie, les mises à jour de routage ne sont pas échangées, sauf en cas de modification de la topologie du réseau. La relation de voisin est maintenue tout au long des paquets Hello. Chaque paquet Hello reçu d'un voisin comprend un temps d'attente. Il s'agit du délai pendant lequel l'ASA peut espérer recevoir un paquet Hello de ce voisin. Si l'ASA ne reçoit pas de paquet Hello de ce voisin dans le délai de rétention annoncé par ce voisin, l'ASA considère que ce voisin n'est pas disponible.

Le protocole EIGRP utilise quatre technologies d'algorithme clés, quatre technologies clés, y compris la découverte et la récupération de voisins, le protocole RTP (Reliable Transport Protocol) et DUAL, ce qui est important pour les calculs de routes. DUAL enregistre toutes les routes vers une destination dans le tableau de topologie et non pas seulement la route la moins coûteuse. La voie de routage la moins coûteuse est insérée dans la table de routage. Les autres routages demeurent dans le tableau de topologie. En cas de défaillance de la voie principale, une autre voie est choisie parmi les successeurs possibles. Un successeur est un routeur voisin utilisé pour le transfert de paquets qui a un chemin à moindre coût vers une destination. Le calcul de faisabilité garantit que le chemin ne fait pas partie d'une boucle de routage.

Si un successeur possible n'est pas trouvé dans le tableau de topologie, un recalcul de la route doit avoir lieu. Lors du recalcul de la route, DUAL interroge les voisins EIGRP pour déterminer une route, qui à leur tour interrogent leurs voisins. Les routeurs qui n'ont pas de successeur possible pour la route renvoient un message d'inaccessibilité.

Lors du recalcul de la route, DUAL marque la route comme active. Par défaut, l'ASA attend trois minutes avant de recevoir une réponse de ses voisins. Si l'ASA ne reçoit pas de réponse d'un voisin, la route est marquée comme bloquée en mode actif. Tous les routages dans le tableau de topologie qui désignent le voisin qui ne répond pas comme un successeur de faisabilité sont supprimés.

Remarque Les relations de voisins EIGRP ne sont pas prises en charge par le tunnel IPsec sans un tunnel GRE.

Null0 et EIGRP

Par défaut, le protocole EIGRP annonce la route Null0 à l'homologue comme route récapitulative pour empêcher le routeur qui annonce le résumé de transférer des paquets n'ayant pas de route.

Par exemple, envisageons les deux routeurs, R1 et R2. Les trois interfaces sur R1 ont ces réseaux : 192.168.0.0/24, 192.168.1.0/24 et 192.168.3.0/24. Configurez R1 avec la route récapitulative 192.168.0.0/22 et annoncez-le à R2. Lorsque R2 a un paquet IP pour 192.168.2.x, il le transmettra à R1. R1 abandonnerait le paquet, car il n'a pas 192.168.2.x dans sa table de routage. Cependant, si R1 est également connecté à un FAI et qu'il a une route par défaut pointant vers le FAI, le paquet 192.168.2.x est transféré au FAI. Pour empêcher cette action de transfert, l'EIGRP génère une entrée correspondant à la route récapitulative, pointant vers Null0. Ainsi, lorsque les paquets pour 192.168.2.x sont reçus, R1 abandonnera le paquet au lieu d'utiliser la route par défaut.

Lignes directrices relatives à l'EIGRP

Directives sur le mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Lignes directrices relatives à la grappe

Le protocole EIGRP ne forme pas de relations de voisinage avec les homologues de la grappe en mode d'interface individuelle.

Directives IPv6

Ne prend pas en charge IPv6.

Lignes directrices relatives au contexte

- Les instances EIGRP ne peuvent pas former de contiguïtés entre elles dans les interfaces partagées car, par défaut, l'échange inter-contextes du trafic de multidiffusion n'est pas pris en charge sur les interfaces partagées. Cependant, vous pouvez utiliser la configuration de voisin statique sous la configuration de processus EIGRP sous le processus EIGRP pour faire apparaître le voisinage EIGRP sur une interface partagée.
- L'EIGRP inter-contexte sur des interfaces distinctes est pris en charge.

Directives de redistribution

Lorsque EIGRP est configuré sur un périphérique qui fait partie du réseau OSPF ou inversement, assurez-vous que le routeur OSPF est configuré pour baliser le routage (EIGRP ne prend pas en charge la balise de routage).

Lors de la redistribution d'EIGRP dans OSPF et d'OSPF dans EIGRP, une boucle de routage se produit en cas de panne sur une des liaisons ou interfaces ou même lorsque l'expéditeur de la route est en panne. Pour empêcher la redistribution des routages d'un domaine vers le même domaine, un routeur peut marquer un routage qui appartient à un domaine pendant qu'il redistribue, et ces routages peuvent être filtrés sur le routeur distant en se basant sur la même balise. Comme les routes ne seront pas installées dans la table de routage, elles ne seront pas redistribuées dans le même domaine.

Directives supplémentaires

- Un maximum d'un processus EIGRP est pris en charge.
- Les intermittences de contiguïté EIGRP se produisent chaque fois qu'une modification de configuration est appliquée, ce qui entraîne une modification des renseignements de routage (envoyés ou reçus) des voisins, en particulier dans les listes de distribution, les listes de décalage et les modifications de récapitulation. Après la synchronisation des routeurs, l'EIGRP rétablit la contiguïté entre les routeurs voisins. Lorsqu'une contiguïté est supprimée et rétablie, toutes les routes apprises entre les voisins sont effacées et la synchronisation complète entre les voisins est nouvellement effectuée avec la nouvelle liste de distribution.
- Il n'y a aucune restriction sur le nombre maximum de voisins EIGRP. Cependant, pour éviter les intermittences EIGRP inutiles, nous vous conseillons de limiter le nombre à 500 par unité.

Configurer un processus EIGRP

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** .

Étape 2 Activez le processus de routage EIGRP en cochant la case **Enable this EIGRP process** (Activer ce processus EIGRP) sous l'onglet Process Instances (Instances de processus). Reportez-vous aux sections Activer EIGRP, à la page 1019 ou Activer le routage Stub EIGRP, à la page 1020.

Étape 3 Définissez les réseaux et les interfaces qui participeront au routage EIGRP sous l'onglet Setup (Configuration) > Networks (Réseaux). Consultez Définir un réseau pour un processus de routage EIGRP, à la page 1021 pour de plus amples renseignements.

Étape 4 (Facultatif) Définissez des filtres de routage dans le volet Filter Rules (Règles de filtre). Le filtrage de routes offre plus de contrôle sur les routes qui peuvent être envoyées ou reçues dans les mises à jour de l'EIGRP. Consultez Filtrer les réseaux dans l'EIGRP, à la page 1030 pour de plus amples renseignements.

Étape 5 (Facultatif) Définissez la redistribution des routes dans le volet Redistribution.

Vous pouvez redistribuer les routes détectées par RIP et OSPF vers le processus de routage EIGRP. Vous pouvez également redistribuer les routes statiques et connectées vers le processus de routage EIGRP. Consultez Redistribuer les routes dans l'EIGRP, à la page 1028 pour de plus amples renseignements.

Étape 6 (Facultatif) Définissez les voisins EIGRP statiques dans le volet Static Neighbor (Voisin statique).

Consultez Définir un voisin EIGRP, à la page 1027 pour de plus amples renseignements.

Étape 7 (Facultatif) Définissez les adresses sommaires dans le volet Summary Address (Adresse sommaire).

Consultez Configurer les adresses d'agrégation du résumé sur les interfaces, à la page 1024 pour en savoir plus sur la définition des adresses sommaires.

Étape 8 (Facultatif) Définissez les paramètres EIGRP spécifiques à l'interface dans le volet Interfaces. Ces paramètres comprennent l'authentification du message EIGRP, le délai de rétention, l'intervalle Hello, la mesure du délai et l'utilisation de l'horizon partagé. Consultez Configurer les interfaces pour l'EIGRP, à la page 1022 pour de plus amples renseignements.

Étape 9 (Facultatif) Contrôlez l'envoi et la réception des informations de routage par défaut dans les mises à jour de l'EIGRP dans le volet Default Information (Informations par défaut). Par défaut, les routes par défaut sont envoyées et acceptées. Consultez Configurer les informations par défaut dans l'EIGRP, à la page 1032 pour de plus amples renseignements.

Configurer le protocole EIGRP

Cette section décrit comment activer le processus EIGRP sur votre système. Après avoir activé l'EIGRP, consultez les sections suivantes pour savoir comment personnaliser le processus EIGRP sur votre système.

Activer EIGRP

Vous ne pouvez activer qu'un seul processus de routage EIGRP sur l'ASA.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page EIGRP Setup (Configuration d'EIGRP) apparaît.

Les trois onglets du volet principal EIGRP Setup (Configuration d'EIGRP) utilisés pour activer l'EIGRP sont les suivants :

- Les onglets Process Instances (Instances de processus) vous permettent d'activer un processus de routage EIGRP pour chaque contexte. Le mode de contexte unique et le mode de contexte multiple sont tous deux pris en charge. Consultez Activer EIGRP, à la page 1019 et Activer le routage Stub EIGRP, à la page 1020 pour en savoir plus.
- Dans les onglets Networks (Réseaux), vous pouvez spécifier les réseaux utilisés par le processus de routage EIGRP. Pour qu'une interface participe au routage EIGRP, elle doit entrer dans la plage d'adresses définie par les entrées de réseau. Pour que les réseaux statiques et connectés directement soient annoncés, ils doivent également entrer dans la plage des entrées de réseau. Consultez Définir un réseau pour un processus de routage EIGRP, à la page 1021 pour de plus amples renseignements.
- Les onglets Passive Interfaces (Interfaces passives) vous permettent de configurer une ou plusieurs interfaces en tant qu'interfaces passives. Dans EIGRP, une interface passive n'envoie ni ne reçoit de mises à jour de routage. Le tableau des interfaces passives répertorie chaque interface configurée comme interface passive.

Étape 2 Cochez la case **Enable this EIGRP process** (Activer ce processus EIGRP).

Vous ne pouvez activer qu'un seul processus de routage EIGRP sur l'appareil. Vous devez saisir un numéro de système autonome (AS) pour le processus de routage dans le champ EIGRP Process (Processus EIGRP) avant de pouvoir enregistrer vos modifications.

Étape 3 Dans le champ EIGRP Process (Processus EIGRP), saisissez le numéro de système autonome (AS) pour le processus EIGRP. Le numéro AS peut être compris entre 1 et 65 535.

Étape 4 (Facultatif) Cliquez sur **Advanced** (Avancé) pour configurer les paramètres du processus EIGRP, tels que l'ID de routeur, les mesures par défaut, le routage de stub, les modifications de voisin et les distances administratives pour les routes EIGRP.

Étape 5 Cliquez sur l'onglet **Networks** (Réseaux).

Étape 6 Pour ajouter une nouvelle entrée de réseau, cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add EIGRP Network** (Ajouter un réseau EIGRP) apparaît. Pour supprimer une entrée de réseau, choisissez une entrée dans le tableau et cliquez sur **Delete** (Supprimer).

Étape 7 Choisissez le numéro AS du processus de routage EIGRP dans la liste déroulante.

Étape 8 Saisissez l'adresse IP des réseaux pour participer au processus de routage EIGRP dans le champ IP Adress (Adresse IP).

Remarque Pour modifier une entrée de réseau, vous devez d'abord supprimer l'entrée, puis en ajouter une nouvelle. Vous ne pouvez pas modifier les entrées existantes.

Étape 9 Saisissez un masque réseau à appliquer à l'adresse IP dans le champ Network Mask (Masque réseau).

Étape 10 Cliquez sur **OK**.

Activer le routage Stub EIGRP

Vous pouvez activer et configurer l'ASA en tant que routeur stub EIGRP. Le routage stub réduit les exigences de mémoire et de traitement sur l'ASA. En tant que routeur stub, l'ASA n'a pas besoin de maintenir une table de routage EIGRP complète, car il transfère tout le trafic non local vers un routeur de distribution. En règle générale, le routeur de distribution n'a pas besoin d'envoyer plus d'une route par défaut au routeur stub.

Seules les routes spécifiées sont propagées du routeur stub au routeur de distribution. En tant que routeur stub, l'ASA répond à toutes les requêtes de résumés, de routes connectées, de routes statiques redistribuées, de routes externes et de routes internes par le message « inaccessible ». Lorsque l'ASA est configuré en tant que stub, il envoie un paquet de renseignements sur les homologues spécial à tous les routeurs voisins pour signaler son état en tant que routeur stub. Tout voisin qui reçoit un paquet pour l'informer de l'état du stub n'interrogera pas le routeur stub sur aucune route, et un routeur qui a un homologue stub n'interrogera pas cet homologue. Le routeur stub dépend du routeur de distribution pour envoyer les mises à jour correctes à tous les homologues.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cochez la case **Enable EIGRP routing** (Activer le routage EIGRP).

Étape 3 Dans le champ **EIGRP Process** (Processus EIGRP), saisissez le numéro de système autonome (AS) pour le processus EIGRP. Le numéro AS peut être compris entre 1 et 65 535.

Étape 4 Cliquez sur **Advanced** (Avancé) pour configurer le processus de routage stub EIGRP.

La boîte de dialogue **Edit EIGRP Process Advanced Properties** (Modifier les propriétés avancées du processus EIGRP) apparaît.

Étape 5 Dans la zone **Stub** de la boîte de dialogue **Edit EIGRP Process Advanced Properties** (Modifier les propriétés avancées du processus EIGRP), choisissez un ou plusieurs des processus de routage stub EIGRP suivants :

- Réception stub uniquement : configure le processus de routage du protocole EIGRP pour recevoir les renseignements de routage des routeurs voisins, mais n'envoie pas de renseignements de routage aux voisins. Si cette option est sélectionnée, vous ne pouvez pas sélectionner les autres options de routage stub.
- Stub connecté : annonce les routes connectées.
- Stub statique : annonce les routes statiques.

- Stub redistribué : annonce les routes redistribuées.
- Résumé du stub : annonce les routes récapitulatives.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur l'onglet **Networks** (Réseaux).

Étape 8 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle entrée de réseau.

La boîte de dialogue **Add EIGRP Network** (Ajouter un réseau EIGRP) apparaît. Pour supprimer une entrée de réseau, choisissez l'entrée dans le tableau et cliquez sur **Delete** (Supprimer).

Étape 9 Choisissez le numéro AS du processus de routage EIGRP dans la liste déroulante.

Étape 10 Saisissez l'adresse IP des réseaux pour participer au processus de routage EIGRP dans le champ **IP Adress** (Adresse IP).



Remarque Pour modifier une entrée de réseau, vous devez d'abord supprimer l'entrée, puis en ajouter une nouvelle. Vous ne pouvez pas modifier les entrées existantes.

Étape 11 Saisissez un masque réseau à appliquer à l'adresse IP dans le champ **Network Mask** (Masque réseau).

Étape 12 Cliquez sur **OK**.

Personnaliser l'EIGRP

Cette section décrit comment personnaliser le routage EIGRP.

Définir un réseau pour un processus de routage EIGRP

Le tableau des réseaux vous permet de spécifier les réseaux utilisés par le processus de routage EIGRP. Pour qu'une interface participe au routage EIGRP, elle doit entrer dans la plage d'adresses définie par les entrées de réseau. Pour que les réseaux statiques et connectés directement soient annoncés, ils doivent également entrer dans la plage des entrées de réseau.

Le tableau des réseaux affiche les réseaux configurés pour le processus de routage EIGRP. Chaque ligne du tableau affiche l'adresse réseau et le masque associé configurés pour le processus de routage EIGRP indiqué.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cochez la case **Enable EIGRP routing** (Activer le routage EIGRP).

Étape 3 Dans le champ **EIGRP Process** (Processus EIGRP), saisissez le numéro de système autonome (AS) pour le processus EIGRP. Le numéro AS peut être compris entre 1 et 65 535.

Étape 4 Cliquez sur l'onglet **Networks** (Réseaux).

Étape 5 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle entrée de réseau.

La boîte de dialogue **Add EIGRP Network** (Ajouter un réseau EIGRP) apparaît. Pour supprimer une entrée de réseau, choisissez l'entrée dans le tableau et cliquez sur **Delete** (Supprimer).

Étape 6 Choisissez le numéro AS du processus de routage EIGRP dans la liste déroulante.

Étape 7 Saisissez l'adresse IP des réseaux pour participer au processus de routage EIGRP dans le champ **IP Adress** (Adresse IP).



Remarque Pour modifier une entrée de réseau, vous devez d'abord supprimer l'entrée, puis en ajouter une nouvelle. Vous ne pouvez pas modifier les entrées existantes.

Étape 8 Saisissez un masque réseau à appliquer à l'adresse IP dans le champ **Network Mask** (Masque réseau).

Étape 9 Cliquez sur **OK**.

Configurer les interfaces pour l'EIGRP

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est connectée à un réseau que vous souhaitez annoncer, vous pouvez configurer l'ASA qui inclut le réseau auquel l'interface est connectée et empêcher cette interface d'envoyer ou de recevoir des mises à jour de l'EIGRP.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cochez la case **Enable EIGRP routing** (Activer le routage EIGRP).

Étape 3 Cliquez sur **OK**.

Étape 4 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Interfaces**.

Le volet **Interface** apparaît et affiche les configurations de l'interface EIGRP. Le tableau **Interface Parameters** (Paramètres d'interface) affiche toutes les interfaces de l'ASA et vous permet de modifier les paramètres suivants par interface :

- Clé et mode d'authentification.
- L'intervalle Hello et le délai de rétention dans l'EIGRP.
- La mesure du délai d'interface utilisée dans les calculs des mesures EIGRP.
- L'utilisation de mode d'horizon partagé sur l'interface.

Étape 5 Choisissez une entrée d'interface en double-cliquant sur une entrée d'interface, ou choisissez l'entrée et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit EIGRP Interface Entry** (Modifier l'entrée de l'interface EIGRP) apparaît.

Étape 6 Dans le champ **EIGRP Process** (Processus EIGRP), saisissez le numéro AS pour le processus EIGRP. Le numéro AS peut aller de 1 à 65 535.

Étape 7 Dans le champ **Hello Interval** (Intervalle Hello), saisissez l'intervalle entre les paquets Hello du protocole EIGRP envoyés sur une interface.

Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.

Étape 8 Dans le champ **Hold Time** (Délai de rétention), saisissez le délai de rétention, en secondes. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est 15secondes.

Étape 9 Cochez la case **Enable** (Activer) pour (Split Horizon) l'horizon partagé.

Étape 10 Dans le champ **Delay** (Délai), saisissez la valeur du délai. Le retard de routage en expimé en dizaines de microsecondes. Les valeurs valides sont comprises entre 1 et 16777215.

Étape 11 Cochez la case **Enable MD5 Authentication** (Activer l'authentification MD5) pour activer l'authentification MD5 des messages de processus EIGRP.

Étape 12 Saisissez les valeurs Key (Clé) ou Key ID (ID de clé).

- Dans le champ **Key** (Clé), saisissez la clé pour authentifier les mises à jour EIGRP. La clé peut contenir jusqu'à 16 caractères.
- Dans le champ **Key ID** (ID de clé), saisissez la valeur d'identification de clé. Les valeurs valides sont comprises entre 0 et 255.

Étape 13 Cliquez sur **OK**.

Configurer des interfaces passives

Vous pouvez configurer une ou plusieurs interfaces en tant qu'interfaces passives. Dans EIGRP, une interface passive n'envoie ni ne reçoit de mises à jour de routage. Dans ASDM, le tableau des interfaces passives répertorie chaque interface configurée en tant qu'interface passive.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cochez la case **Enable EIGRP routing** (Activer le routage EIGRP).

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur l'onglet **Passive Interfaces** (Interfaces passives).

Étape 5 Choisissez l'interface que vous souhaitez configurer dans la liste déroulante.

Étape 6 Cochez la case **Suppress routing updates on all interfaces** (Supprimer les mises à jour de routage sur toutes les interfaces) pour indiquer que toutes les interfaces sont passives. Même si une interface n'est pas affichée dans le tableau des interfaces passives, elle sera configurée comme passive lorsque la case sera cochée.

Étape 7 Cliquez sur **Add** (Ajouter) pour ajouter une entrée d'interface passive.

La boîte de dialogue **Add EIGRP Passive Interface** (Ajouter une interface passive EIGRP) apparaît. Choisissez l'interface que vous souhaitez rendre passive, puis cliquez sur **Add** (Ajouter). Pour supprimer une interface passive, choisissez l'interface dans le tableau et cliquez sur **Delete** (Supprimer).

Étape 8 Cliquez sur **OK**.

Configurer les adresses d'agrégation du résumé sur les interfaces

Vous pouvez configurer une adresse sommaire pour chaque interface. Vous devez définir manuellement les adresses sommaires si vous souhaitez créer des adresses sommaires qui ne se produisent pas à la limite d'un numéro de réseau, ou si vous souhaitez utiliser des adresses sommaires sur l'ASA avec le récapitulatif de routage automatique désactivé. Si des routes plus spécifiques se trouvent dans la table de routage, EIGRP annoncera l'adresse sommaire hors de l'interface avec une mesure égale au minimum de toutes les routes plus spécifiques.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Interfaces**.

Le volet **Interface** affiche les configurations de l'interface EIGRP. Le tableau Interface Parameters (Paramètres d'interface) présente toutes les interfaces de l'ASA et vous permet de modifier les paramètres par interface. Pour plus de renseignements sur ces paramètres, consultez Configurer les interfaces pour l'EIGRP, à la page 1022.

Étape 2 Pour configurer les paramètres EIGRP pour une interface, cliquez deux fois sur une entrée d'interface ou sélectionnez l'entrée et cliquez sur **Edit** (Modifier).

Étape 3 Cliquez sur **OK**.

Étape 4 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Summary Address (Adresse sommaire)**.

Le volet **Summary Address** (Adresse sommaire) affiche un tableau des adresses sommaires EIGRP définies de manière statique. Par défaut, EIGRP résume les routes de sous-réseau au niveau du réseau. Vous pouvez créer des adresses sommaires EIGRP définies statiquement au niveau du sous-réseau à partir du volet **Summary Address** (Adresse sommaire).

Étape 5 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle adresse sommaire EIGRP ou sur **Edit** (Modifier) pour modifier une adresse sommaire EIGRP existante dans le tableau.

La boîte de dialogue **Add Summary Address** (Ajouter une adresse sommaire) ou **Edit Summary Address** (Modifier une adresse sommaire) apparaît. Vous pouvez également cliquer deux fois sur une entrée du tableau pour la modifier.

Étape 6 Dans le champ **EIGRP Process** (Processus EIGRP), saisissez le numéro de système autonome (AS) pour le processus EIGRP. Le numéro AS peut être compris entre 1 et 65 535.

Étape 7 Dans la liste déroulante **Interface**, choisissez l'interface à partir de laquelle l'adresse sommaire est annoncée.

Étape 8 Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de la route récapitulative.

Étape 9 Dans le champ **Netmask** (Masque réseau), choisissez ou saisissez le masque réseau à appliquer à l'adresse IP.

Étape 10 Saisissez la distance administrative pour la route dans le champ **Administrative Distance** (Distance administrative). Si ce champ est laissé vide, la distance administrative par défaut de 5 est attribuée à la route.

Étape 11 Cliquez sur **OK**.

Modifier la valeur du délai d'interface

La valeur du délai d'interface est utilisée dans les calculs de distance EIGRP. Vous pouvez modifier cette valeur par interface.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Interface**.

Le volet **Interface** affiche les configurations de l'interface EIGRP. Le tableau **Interface Parameters** (Paramètres d'interface) présente toutes les interfaces de l'ASA et vous permet de modifier les paramètres par interface. Pour plus de renseignements sur ces paramètres, consultez Configurer les interfaces pour l'EIGRP, à la page 1022.

Étape 2 Effectuez un double clic sur une entrée d'interface ou sélectionnez l'entrée Interface, puis cliquez sur **Edit** (Modifier) pour configurer la valeur de délai dans les paramètres EIGRP pour une interface.

La boîte de dialogue **Edit EIGRP Interface Entry** (Modifier l'entrée de l'interface EIGRP) apparaît.

Étape 3 Dans le champ **Delay** (Délai), saisissez le délai, exprimé en dizaines de microsecondes. Cette valeur peut être comprise entre 1 et 16 777 215.

Étape 4 Cliquez sur **OK**.

Activer l'authentification EIGRP sur une interface

L'authentification de route EIGRP fournit une authentification MD5 des mises à jour de routage provenant du protocole de routage EIGRP. Le condensé de clé MD5 dans chaque paquet EIGRP empêche l'introduction de messages de routage non autorisés ou faux provenant de sources non approuvées.

L'authentification de route EIGRP est configurée par interface. Tous les voisins EIGRP sur les interfaces configurées pour l'authentification des messages EIGRP doivent être configurés avec le même mode d'authentification et la même clé pour que les contiguïtés soient établies.

Remarque Avant de pouvoir activer l'authentification de routage EIGRP, vous devez activer EIGRP.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cochez la case **Enable EIGRP routing** (Activer le routage EIGRP).

Étape 3 Dans le champ **EIGRP Process** (Processus EIGRP), saisissez le numéro de système autonome (AS) pour le processus EIGRP. Le numéro AS peut aller de 1 à 65 535.

Étape 4 Cliquez sur l'onglet **Networks** (Réseaux).

Étape 5 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle entrée de réseau.

La boîte de dialogue **Add EIGRP Network** (Ajouter un réseau EIGRP) apparaît. Pour supprimer une entrée de réseau, choisissez l'entrée dans le tableau et cliquez sur **Delete** (Supprimer).

Étape 6 Choisissez le numéro AS du processus de routage EIGRP dans la liste déroulante.

Étape 7 Dans le champ **IP Adress** (Adresse IP), saisissez l'adresse IP des réseaux pour participer au processus de routage EIGRP.

Remarque Pour modifier une entrée de réseau, vous devez d'abord supprimer l'entrée, puis en ajouter une nouvelle. Vous ne pouvez pas modifier les entrées existantes.

Étape 8 Dans le champ **Network Mask** (Masque réseau), choisissez ou saisissez un masque réseau à appliquer à l'adresse IP.

Étape 9 Cliquez sur **OK**.

Étape 10 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Interfaces**.

Le volet **Interface** affiche les configurations de l'interface EIGRP. Le tableau **Interface Parameters** (Paramètres d'interface) affiche toutes les interfaces de l'ASA et vous permet de modifier les paramètres par interface. Pour plus de renseignements sur ces paramètres, consultez Configurer les interfaces pour l'EIGRP, à la page 1022.

Étape 11 Cochez la case **Enable MD5 Authentication** (Activer l'authentification MD5) pour activer l'authentification MD5 des messages de processus EIGRP. Après avoir coché cette case, effectuez l'une des opérations suivantes :

- Dans le champ **Key** (Clé), saisissez la clé pour authentifier les mises à jour EIGRP. La clé peut inclure jusqu'à 16 caractères.
- Dans le champ **Key ID** (ID de clé), saisissez la valeur d'identification de clé. Les valeurs valides sont comprises entre 0 et 255.

Étape 12 Cliquez sur **OK**.

Définir un voisin EIGRP

Les paquets Hello EIGRP sont envoyés en tant que paquets de multidiffusion. Si un voisin EIGRP se trouve sur un réseau de non-diffusion, comme un tunnel, vous devez définir manuellement ce voisin. Lorsque vous définissez manuellement un voisin EIGRP, les paquets Hello sont envoyés à ce voisin sous forme de messages de monodiffusion.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cochez la case **Enable EIGRP routing** (Activer le routage EIGRP).

Étape 3 Dans le champ **EIGRP Process** (Processus EIGRP), saisissez le numéro AS pour le processus EIGRP. Le numéro AS peut aller de 1 à 65 535.

Étape 4 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Static Neighbor (Voisin statique)**.

Le volet **Static Neighbor** (Voisin statique) apparaît et affiche les voisins EIGRP définis de manière statique. Un voisin EIGRP envoie des renseignements de routage EIGRP à l'ASA et reçoit des renseignements de routage EIGRP de celui-ci. Normalement, les voisins sont découverts de manière dynamique par le biais du processus de découverte de voisins. Cependant, sur les réseaux point à point et sans diffusion, vous devez définir les voisins de manière statique.

Chaque ligne du tableau **Static Neighbor** (Voisin statique) affiche le numéro de système autonome EIGRP pour le voisin, l'adresse IP du voisin et l'interface par laquelle le voisin est disponible.

Dans le volet **Static Neighbor** (Voisin statique), vous pouvez ajouter ou modifier un voisin statique.

Étape 5 Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour ajouter ou modifier un voisin statique EIGRP.

La boîte de dialogue **Add** or **Edit EIGRP Neighbor Entry** (Ajouter ou modifier une entrée de voisin EIGRP) apparaît.

Étape 6 Choisissez le numéro **EIGRP AS** (AS EIGRP) dans la liste déroulante pour le processus EIGRP pour lequel le voisin est configuré.

Étape 7 Choisissez le **Interface Name** (Nom de l'interface) dans la liste déroulante **Interface Name** (Nom de l'interface), qui correspond à l'interface par laquelle le voisin est disponible.

Étape 8 Dans le champ **Neighbor IP Address** (Adresse IP du voisin), saisissez l'adresse IP du voisin.

Étape 9 Cliquez sur **OK**.

Redistribuer les routes dans l'EIGRP

Vous pouvez redistribuer les routes détectées par RIP et OSPF dans le processus de routage EIGRP. Vous pouvez également redistribuer les routes statiques et connectées dans le processus de routage EIGRP. Vous n'avez pas besoin de redistribuer les routes connectées si elles entrent dans la plage d'une instruction **network** dans la configuration EIGRP.



Remarque Pour le protocole RIP uniquement : avant d'entamer cette procédure, vous devez créer une carte de routage pour définir plus précisément quelles routes du protocole de routage spécifié sont redistribuées dans le processus de routage RIP.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cochez la case **Enable EIGRP routing** (Activer le routage EIGRP).

Étape 3 Dans le champ **EIGRP Process** (Processus EIGRP), saisissez le numéro AS pour le processus EIGRP. Le numéro AS peut aller de 1 à 65 535.

Étape 4 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Redistribution**.

Le volet **Redistribution** affiche les règles de redistribution des routes à partir d'autres protocoles de routage vers le processus de routage EIGRP. Lors de la redistribution des routes statiques et connectées au processus de routage EIGRP, il n'est pas nécessaire de configurer des mesures, bien que cela soit conseillé. Chaque ligne du tableau du volet **Redistribution** comprend une entrée de redistribution des routes.

Étape 5 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle règle de redistribution. Si vous modifiez une règle de redistribution existante, passez à l'étape 6.

La boîte de dialogue **Add EIGRP Redistribution Entry** (Ajouter une entrée de redistribution EIGRP) apparaît.

Étape 6 Choisissez l'adresse dans le tableau et cliquez sur **Edit** (Modifier) pour modifier un voisin statique EIGRP existant. Vous pouvez également cliquer deux fois sur une entrée du tableau pour modifier cette entrée.

La boîte de dialogue **Edit EIGRP Redistribution Entry** (Modifier une entrée de redistribution EIGRP) apparaît.

Étape 7 Choisissez le numéro AS du processus de routage EIGRP auquel l'entrée s'applique dans la liste déroulante.

Étape 8 Dans la zone **Protocol** (Protocole), cliquez sur le bouton radio à côté de l'un des protocoles suivants pour le processus de routage :

- **Static** (Statique) pour redistribuer les routes statiques vers le processus de routage EIGRP. Les routes statiques qui entrent dans la portée d'un relevé du réseau sont automatiquement redistribuées dans EIGRP; vous n'avez pas besoin de définir de règle de redistribution les concernant.

- **Connected** (Connecté) pour redistribuer les routes connectées dans le processus de routage EIGRP. Les routes connectées qui entrent dans la portée d'un relevé de réseau sont automatiquement redistribuées dans EIGRP; vous n'avez pas besoin de définir de règle de redistribution les concernant.
- **RIP** pour redistribuer les routes détectées par le processus de routage RIP vers le protocole EIGRP.
- **OSPF** pour redistribuer les routes détectées par le processus de routage OSPF vers le protocole EIGRP.

Étape 9 Dans la zone **Optional Metrics** (Mesures facultatives), choisissez l'une des mesures suivantes utilisées pour la route redistribuée :

- **Bandwidth** (Bande passante), qui est la mesure de la bande passante de l'EIGRP en kilobits par seconde. Les valeurs valides sont comprises entre 0 et 4294967294.
- **Delay** (Délai), qui est la mesure du délai de l'EIGRP en unités de 10 microsecondes. Les valeurs valides vont de 0 à 4294967295.
- **Reliability** (Fiabilité), qui est la mesure de fiabilité de l'EIGRP. Les valeurs valides vont de 0 à 255; la valeur 255 indique une fiabilité à 100 %.
- **Loading** (Chargement), qui est la mesure de la bande passante efficace (chargement) de l'EIGRP. Les valeurs valides vont de 1 à 255; la valeur 255 indique un chargement à 100 %.
- **MTU**, qui est la MTU du chemin. Cette valeur peut être comprise entre 1 et 65 535.

Étape 10 Choisissez la carte de routage dans la liste déroulante **Route Map** (Carte de routage) pour définir quelles routes sont redistribuées dans le processus de routage EIGRP. Pour plus de détails sur la configuration d'une carte de routage, consultez Cartes de routage, à la page 883.

Étape 11 Dans la zone **Optional OSPF Redistribution** (Redistribution OSPF facultative), cliquez sur l'un des boutons radio OSPF suivants pour indiquer plus précisément quelles routes OSPF sont redistribuées dans le processus de routage EIGRP :

- **Match Internal** (Correspondance interne) pour faire correspondre les routes internes au processus OSPF spécifié.
- **Match External 1** (Correspondance externe 1) pour faire correspondre les routes de type 1 externes au processus OSPF spécifié.
- **Match External 2** (Correspondance externe 2) pour faire correspondre les routes de type 2 externes au processus OSPF spécifié.
- **Match NSSA-External 1** (Correspondance NSSA-externe 1) pour faire correspondre les routes de type 1 externes au NSSA OSPF spécifié.
- **Match NSSA-External 2** (Correspondance NSSA-externe 2) pour faire correspondre les routes de type 2 externes au NSSA OSPF spécifié.

Étape 12 Cliquez sur **OK**.

Filtrer les réseaux dans l'EIGRP

Remarque Avant de commencer ce processus, vous devez créer une ACL standard qui définit les routes que vous souhaitez annoncer. C'est-à-dire que vous créez une ACL standard qui définit les routes que vous souhaitez filtrer à partir de l'envoi ou de la réception des mises à jour.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cochez la case **Enable EIGRP routing** (Activer le routage EIGRP).

Étape 3 Dans le champ **EIGRP Process** (Processus EIGRP), saisissez le numéro AS pour le processus EIGRP. Le numéro AS peut aller de 1 à 65 535.

Étape 4 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Filter Rules (Règles de filtre)**.

Le volet **Filter Rules** (Règles de filtre) apparaît et affiche les règles de filtrage des routes configurées pour le processus de routage EIGRP. Les règles de filtre vous permettent de contrôler les routes acceptées ou annoncées par le processus de routage EIGRP.

Chaque ligne du tableau **Filter Rule** (Règle de filtre) décrit une règle de filtre pour une interface ou un protocole de routage spécifique. Par exemple, une règle de filtre avec une direction d'entrée sur l'interface externe appliquera le filtrage à toutes les mises à jour EIGRP reçues sur l'interface externe. Une règle de filtre avec une direction de sortie et OSPF 10 spécifié comme protocole de routage appliquera les règles de filtre aux routes redistribuées dans le processus de routage EIGRP dans les mises à jour EIGRP sortantes.

Étape 5 Cliquez sur **Add** (Ajouter) pour ajouter une règle de filtre. Si vous modifiez une règle de filtre déjà existante, passez à l'étape 6.

La boîte de dialogue **Add Filter Rules** (Ajouter des règles de filtre) apparaît.

Étape 6 Pour modifier une règle de filtre, choisissez la règle de filtre dans le tableau et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Filter Rules** (Modifier les règles de filtre) apparaît. Vous pouvez également cliquer deux fois sur une règle de filtre pour modifier la règle. Pour supprimer une règle de filtre, choisissez la règle de filtre dans le tableau et cliquez sur **Delete** (Supprimer).

Étape 7 Choisissez le numéro AS dans la liste déroulante du processus de routage EIGRP auquel l'entrée s'applique.

Étape 8 Dans la liste déroulante, choisissez la direction des routes de filtre.

Choisissez **in** (entrée) pour les règles qui filtrent les routes à partir des mises à jour de routage EIGRP entrantes. Choisissez **out** (sortie) pour filtrer les routes à partir des mises à jour de routage EIGRP envoyées par l'ASA.

Si vous choisissez **out** (sortie), le champ de processus **Routing** (Routage) devient actif. Choisissez le type de route à filtrer. Vous pouvez filtrer les routes redistribuées à partir des processus de routage statiques, connectés, RIP et OSPF. Les filtres qui spécifient un processus de routage filtrent les routes à partir des mises à jour envoyées sur toutes les interfaces.

Étape 9 Saisissez l'ID du processus OSPF dans le champ **ID**.

Étape 10 Cliquez sur le bouton radio **Interface** et choisissez l'interface à laquelle le filtre s'applique.

Étape 11 Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour définir une ACL pour la règle de filtre. Cliquez sur **Edit** (Modifier) pour ouvrir la boîte de dialogue **Network Rule** (Règle de réseau) pour la règle de réseau sélectionnée.

Étape 12 Dans la liste déroulante **Action**, sélectionnez **Permit** (Autoriser) pour autoriser l'annonce du réseau spécifié; choisissez **Deny** (Refuser) pour empêcher le réseau spécifié d'être annoncé.

Étape 13 Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP du réseau autorisée ou refusée. Pour autoriser ou refuser toutes les adresses, utilisez l'adresse IP **0.0.0.0** avec le masque réseau **0.0.0.0**.

Étape 14 Dans la liste déroulante **Netmask** (Masque réseau), choisissez le masque réseau appliqué à l'adresse IP du réseau. Vous pouvez saisir un masque réseau dans ce champ ou sélectionner l'un des masques courants dans la liste.

Étape 15 Cliquez sur **OK**.

Personnaliser l'intervalle Hello et le délai de rétention dans l'EIGRP

L'ASA envoie périodiquement des paquets Hello pour découvrir les voisins et savoir quand ceux-ci deviennent inaccessibles ou inopérants. Par défaut, les paquets Hello sont envoyés toutes les 5 secondes.

Le paquet Hello annonce le délai de rétention de l'ASA. Le délai de rétention indique aux voisins EIGRP la durée pendant laquelle le voisin doit considérer l'ASA comme accessible. Si le voisin ne reçoit pas de paquet Hello dans le délai de rétention annoncé, l'ASA est considéré comme inaccessible. Par défaut, le délai de rétention annoncé est de 15 secondes (trois fois l'intervalle Hello).

L'intervalle Hello et le délai de rétention annoncé sont configurés par interface. Nous vous conseillons de définir le délai de rétention à au moins trois fois l'intervalle Hello.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cochez la case **Enable EIGRP routing** (Activer le routage EIGRP).

Étape 3 Cliquez sur **OK**.

Étape 4 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Interfaces**.

Le volet **Interface** apparaît et affiche toutes les configurations d'interface EIGRP.

Étape 5 Cliquez deux fois sur une entrée d'interface ou choisissez l'entrée et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit EIGRP Interface Entry** (Modifier l'entrée de l'interface EIGRP) apparaît.

Étape 6 Choisissez le numéro AS EIGRP dans la liste déroulante, qui est renseignée à partir des numéros système configurés lorsque vous avez activé le processus de routage EIGRP.

Étape 7 Dans le champ **Hello Interval** (Intervalle Hello), saisissez l'intervalle entre les paquets Hello du protocole EIGRP envoyés sur une interface.

Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.

Étape 8 Dans le champ **Hold Time** (Délai de rétention), spécifiez le délai de rétention, en secondes.

Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est 15secondes.

Étape 9 Cliquez sur **OK**.

Désactiver la synthèse automatique des routes

La synthèse automatique des routes est activée par défaut. Le processus de routage par EIGRP se résume sur les limites des numéros de réseau. Cela eut entraîner des problèmes de routage si vous avez des réseaux non contigus.

Par exemple, si vous avez un routeur avec les réseaux 192.168.1.0, 192.168.2.0 et 192.168.3.0 qui y sont connectés et que ces réseaux participent tous à l'EIGRP, le processus de routage EIGRP crée l'adresse sommaire 192.168.0.0 pour ces routes. Si un routeur supplémentaire est ajouté au réseau avec les réseaux 192.168.10.0 et 192.168.11.0 et que ces réseaux participent à l'EIGRP, ils seront également résumés sous la forme 192.168.0.0. Pour éviter que le trafic ne soit acheminé vers le mauvais emplacement, vous devez désactiver la synthèse automatique des routes sur les routeurs qui créent des adresses sommaires conflictuelles.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cochez la case **Enable EIGRP routing** (Activer le routage EIGRP).

Étape 3 Cliquez sur l'onglet **Process Instance** (Instance de processus).

Étape 4 Cliquez sur **Advanced** (Avancé).

Étape 5 Dans la zone **Summary** (Résumé), décochez la case **Auto-Summary** (Résumé automatique).

Remarque Ce paramètre est activé par défaut.

Étape 6 Cliquez sur **OK**.

Configurer les informations par défaut dans l'EIGRP

Vous pouvez contrôler l'envoi et la réception des renseignements sur la route par défaut dans les mises à jour EIGRP. Par défaut, les routes par défaut sont envoyées et acceptées. La configuration de l'ASA pour interdire la réception des renseignements par défaut entraîne le blocage du bit de route par défaut possible sur les routes reçues. La configuration de l'ASA pour interdire l'envoi des renseignements par défaut désactive le réglage du bit de route par défaut dans les routes annoncées.

Dans ASDM, le volet Default Information (Renseignements par défaut) affiche un tableau de règles pour contrôler l'envoi et la réception des renseignements sur les routes par défaut dans les mises à jour EIGRP. Vous pouvez avoir une règle d'entrée et une règle de sortie pour chaque processus de routage EIGRP (un seul processus est actuellement pris en charge).

Par défaut, les routes par défaut sont envoyées et acceptées. Pour restreindre ou désactiver l'envoi et la réception des renseignements sur la route par défaut, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La volet principal **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cochez la case **Enable EIGRP routing** (Activer le routage EIGRP).

Étape 3 Cliquez sur **OK**.

Étape 4 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour créer une nouvelle entrée.
- Pour modifier une entrée, cliquez deux fois sur l'entrée dans le tableau ou sélectionnez une entrée dans le tableau et cliquez sur **Edit** (Modifier).

  La boîte de dialogue **Add Default Information** (Ajouter les renseignements par défaut) ou **Edit Default Information** (Modifier les renseignements par défaut) s'affiche pour cette entrée. Le numéro AS EIGRP est automatiquement sélectionné dans le champ EIGRP.

Étape 5 Dans le champ **Direction**, choisissez la direction de la règle parmi les options suivantes :

- **in** : la règle filtre les renseignements de routage par défaut des mises à jour EIGRP entrantes.
- **out** : la règle filtre les renseignements de routage par défaut des mises à jour EIGRP sortantes.

Vous pouvez avoir une règle d'entrée et une règle de sortie pour chaque processus EIGRP.

Étape 6 Ajoutez des règles de réseau au tableau des règles de réseau. Les règles de réseau définissent les réseaux autorisés et non autorisés lors de la réception ou de l'envoi des renseignements de routage par défaut. Répétez les étapes suivantes pour chaque règle de réseau que vous ajoutez à la règle de filtre des renseignements par défaut.

a) Cliquez sur **Add** (Ajouter) pour ajouter une règle de réseau. Cliquez deux fois sur une règle de réseau existante pour modifier la règle.

b) Dans le champ **Action**, cliquez sur **Allow** (Autoriser) pour autoriser le réseau ou sur **Deny** (Refuser) pour bloquer le réseau.

c) Saisissez l'adresse IP et le masque réseau du réseau autorisé ou refusé par la règle dans les champs IP Address (Adresse IP) et Network Mask (Masque réseau).

   Pour refuser l'acceptation ou l'envoi de tous les renseignements de routage par défaut, saisissez **0.0.0.0** comme adresse réseau et choisissez **0.0.0.0** comme masque réseau.

d) Cliquez sur **OK** pour ajouter la règle de réseau spécifiée à la règle de filtre des renseignements par défaut.

Étape 7 Cliquez sur **OK** pour accepter la règle de filtre des renseignements par défaut.

Désactiver l'horizon divisé de l'EIGRP

L'horizon partagé contrôle l'envoi des paquets de mise à jour et de requête de l'EIGRP. Lorsque l'horizon partagé est activé sur une interface, les paquets de mise à jour et de requête ne sont pas envoyés vers les destinations pour lesquelles cette interface est le prochain saut. Le contrôle des paquets de mise à jour et de requête de cette manière réduit le risque de boucles de routage.

Par défaut, l'horizon partagé est activé sur toutes les interfaces.

L'horizon partagé empêche les renseignements de routage d'être annoncés par un routeur à partir de toute interface d'où proviennent ces renseignements. Ce comportement optimise généralement les communications entre plusieurs périphériques de routage, en particulier lorsque des liaisons sont rompues. Cependant, avec les réseaux de non-diffusion, il peut arriver que ce comportement ne soit pas souhaitable. Pour ces situations, y compris les réseaux dans lesquels vous avez configuré l'EIGRP, vous pouvez désactiver l'horizon partagé.

Si vous désactivez l'horizon partagé sur une interface, vous devez le désactiver pour tous les routeurs et les serveurs d'accès sur cette interface.

Pour désactiver l'horizon partagé de l'EIGRP, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Interface**.

Le volet **Interface** apparaît et affiche les configurations de l'interface EIGRP.

Étape 2 Cliquez deux fois sur une entrée d'interface ou choisissez l'entrée et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit EIGRP Interface Entry** (Modifier l'entrée de l'interface EIGRP) (Modifier l'entrée de l'interface EIGRP) (EIGRPv6) s'affiche.

Étape 3 Choisissez le numéro de système autonome (AS) EIGRP dans la liste déroulante, qui est renseignée à partir des numéros système configurés lorsque vous avez activé le processus de routage EIGRP.

Étape 4 Décochez la case **Split Horizon** (Horizon partagé).

Étape 5 Cliquez sur **OK**.

Redémarrer le processus EIGRP

Vous pouvez redémarrer un processus EIGRP ou effacer la redistribution ou les compteurs.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP** > **Setup (Configuration)**.

La page **EIGRP Setup** (Configuration d'EIGRP) apparaît.

Étape 2 Cliquez sur **Reset** (Réinitialiser).

Supervision de l'EIGRP

Vous pouvez utiliser les commandes suivantes pour superviser le processus de routage EIGRP. Pour obtenir des exemples et des descriptions de la sortie de la commande, consultez la référence de commande. En outre, vous pouvez désactiver la journalisation des messages de modification de voisin et des messages d'avertissement de voisin.

Pour superviser ou désactiver diverses statistiques de routage EIGRP, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **EIGRP Neighbor (Voisin EIGRP)**.

Chaque ligne représente un voisin EIGRP. Pour chaque voisin, la liste comprend son adresse IP, l'interface à laquelle le voisin est connecté, le délai de rétention, le temps de disponibilité, la longueur de la file d'attente, le numéro de séquence, le temps d'aller-retour progressif et le délai d'expiration de la retransmission. Voici une liste des changements d'état possibles :

- NOUVELLE CONTIGUÏTÉ : un nouveau voisin a été établi.
- REDÉMARRAGE DE L'HOMOLOGUE : l'autre voisin initie la réinitialisation de la relation de voisinage. Le routeur qui reçoit le message n'est pas celui qui réinitialise le voisin.
- DÉLAI D'ATTENTE EXPIRÉ : le routeur n'a reçu aucun paquet EIGRP du voisin dans la limite du délai de rétention.
- LIMITE DE NOUVELLES TENTATIVES DÉPASSÉE : EIGRP n'a pas reçu d'accusé de réception du voisin pour les paquets EIGRP fiables, et EIGRP a déjà essayé de retransmettre le paquet fiable 16 fois sans succès.
- FILTRE DE ROUTE MODIFIÉ : le voisin EIGRP se réinitialise en raison d'une modification du filtre de route.
- DÉLAI D'INTERFACE MODIFIÉ : le voisin EIGRP se réinitialise en raison d'une modification manuelle de la configuration du paramètre de délai sur l'interface.
- BANDE PASSANTE D'INTERFACE MODIFIÉE : le voisin EIGRP se réinitialise en raison d'une modification manuelle de la configuration de la bande passante de l'interface.

- BLOQUÉ À L'ÉTAT ACTIF : le voisin EIGRP se réinitialise car EIGRP est bloqué à l'état actif. La réinitialisation du voisin est le résultat de l'état bloqué en mode actif.

Étape 2 Cliquez sur le voisin EIGRP que vous souhaitez superviser.

Étape 3 Pour supprimer la liste actuelle des voisins, cliquez sur **Clear Neighbors** (Effacer les voisins).

Étape 4 Pour actualiser la liste actuelle des voisins, cliquez sur **Refresh** (Actualiser).

Remarque Par défaut, les messages de modification de voisin et d'avertissement de voisin sont enregistrés.

Historique d'EIGRP

Tableau 44 : Historique des fonctionnalités d'EIGRP

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge d'EIGRP	7.0(1)	Une prise en charge a été ajoutée pour le routage des données, l'exécution de l'authentification, ainsi que la redistribution et la supervision des informations de routage à l'aide du protocole EIGRP (Enhanced Interior Gateway Routing Protocol). Nous avons introduit l'écran suivant : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **EIGRP**.
Routage dynamique en mode de contexte multiple	9.0(1)	Le routage EIGRP est pris en charge en mode de contexte multiple. Nous avons modifié l'écran suivant : **Configuration** > **Device Setup (Configuration du périphérique)** > **Routing (Routage)** > **EIGRP** > **Setup** (Configuration).
Mise en grappe	9.0(1)	Pour l'EIGRP, la synchronisation groupée, la synchronisation du routage et l'équilibrage de charges de couche 2 sont pris en charge dans l'environnement de mise en grappe.
Champ Auto-Summary (Résumé automatique) de l'EIGRP	9.2(1)	Pour l'EIGRP, le champ Auto-Summary (Résumé automatique) est maintenant désactivé par défaut. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > EIGRP > Configuration > Edit EIGRP Process Advanced Properties (Modifier les propriétés avancées du processus EIGRP).



CHAPITRE 37

Routage multidiffusion

Ce chapitre décrit comment configurer ASA pour utiliser le protocole de routage de multidiffusion.

- Routage multidiffusion, à la page 1037
- Lignes directrices pour le routage de multidiffusion, à la page 1041
- Routage multidiffusion activé, à la page 1042
- Personnaliser le routage multidiffusion, à la page 1043
- Supervision de PIM, à la page 1059
- Exemple de routage de multidiffusion, à la page 1059
- Historique du routage de multidiffusion, à la page 1061

Routage multidiffusion

Le routage de multidiffusion est une technologie de conservation de la bande passante qui réduit le trafic en délivrant simultanément un seul flux d'informations à des milliers d'entreprises et de domiciles. Les applications comprennent les vidéoconférences, les communications d'entreprise, l'apprentissage à distance et la distribution de logiciels, de cotations boursières et d'actualités.

Applications et protocoles de routage de multidiffusion

Les protocoles de routage de multidiffusion envoient efficacement le trafic source à plusieurs destinataires, sans ajouter de charge supplémentaire sur la source ou les destinataires, et utilisent moins de bande passante réseau que les autres technologies. Les paquets en multidiffusion sont répliqués dans le réseau par l'activation de l'ASA avec PIM (Protocol Independent Multicast) et d'autres protocoles de multidiffusion qui prennent en charge, ce qui permet la livraison la plus efficace possible des données à plusieurs destinataires.

L'ASA prend en charge le routage de multidiffusion stub et le routage de multidiffusion PIM. Cependant, vous ne pouvez pas configurer les deux simultanément sur un seul ASA.

Remarque Les transports UDP et non-UDP sont tous deux pris en charge pour le routage de multidiffusion. Cependant, le transport non UDP n'a pas d'optimisation FastPath.

Routage de multidiffusion en mode stub

Le routage de multidiffusion tampon permet un enregistrement dynamique de l'hôte et facilite le routage de multidiffusion.

Lorsqu'il est configuré pour le routage de multidiffusion stub, l'ASA agit comme un agent mandataire IGMP. Au lieu de participer entièrement au routage de multidiffusion, l'ASA transfère les messages IGMP à un routeur de multidiffusion en amont, qui configure la livraison des données en multidiffusion. Lorsqu'il est configuré pour le routage de multidiffusion tampon, l'ASA ne peut pas être configuré pour le mode PIM discret ou bidirectionnel. Activez PIM sur les interfaces qui participent au routage de multidiffusion en mode stub IGMP.

L'ASA prend en charge PIM-SM et PIM bidirectionnel. PIM-SM est un protocole de routage de multidiffusion qui utilise la base d'information de routage sous-jacente de monodiffusion ou une base d'information de routage distincte compatible avec la multidiffusion. Il crée des arborescences partagées unidirectionnelles, chacune ayant pour racine un seul point de rendez-vous (PRV) par groupe de multidiffusion. Il crée éventuellement des arborescences de plus court chemin pour chaque source de multidiffusion.

Routage de multidiffusion PIM

Le PIM bidirectionnel est une variante de PIM-SM qui crée des arborescences partagées bidirectionnelles connectant les sources et les récepteurs de multidiffusion.

Processus d'élection du DF

Les arborescences bidirectionnelles sont créées à l'aide d'un processus de sélection de désigné de transitaire (DF) qui fonctionne sur chaque lien de la topologie de multidiffusion. Avec l'aide du DF, les données en multidiffusion sont transmises des sources au point de rendez-vous (RP), et donc le long de l'arborescence partagée jusqu'aux récepteurs. Ce processus ne nécessite pas d'état spécifique à la source. Le choix du DF a lieu lors de la découverte du RP et fournit une voie de routage par défaut vers le RP.



Remarque Si ASA est le RP du PIM, utilisez l'adresse externe non traduite de l'ASA comme adresse RP.

Mode PIM clairsemé

Le mode clairsemé (PIM-SM) est un mode PIM qui transfère le trafic uniquement lorsqu'il est spécifiquement demandé par les destinataires. Il utilise un point de rendez-vous (PRV) central pour coordonner le transfert du trafic de multidiffusion entre la source de multidiffusion et la destination. Le PRV est un routeur qui sert de point de rencontre pour la source et les destinataires. Les sources de multidiffusion s'enregistrent auprès du PRV par l'intermédiaire de leur routeur de premier saut. Ils envoient une copie du trafic de multidiffusion aux destinataires par l'intermédiaire du PRV.

Prise en charge de la multidiffusion PIM propre à la source

ASA peut transférer le trafic de multidiffusion spécifique à la source (p. ex., pour les groupes dans la plage 232.xxx) même s'il ne prend pas en charge la configuration PIM-SSM ou le protocole de gestion de groupes Internet version 3 (IGMPv3).

SSM est classé comme un mécanisme de livraison de données pour les applications un-à-plusieurs telles que l'IPTV. Le modèle SSM utilise un concept de « canaux » désigné par une paire (S, G), où S est une adresse de source et G une adresse de destination SSM. L'abonnement à un canal se fait à l'aide d'un protocole de gestion de groupe comme IGMPv3. SSM permet à un client destinataire, une fois qu'il a pris connaissance d'une source en multidiffusion particulière, de recevoir des flux en multidiffusion directement de la source plutôt que de les recevoir d'un point de rendez-vous partagé (RP). Des mécanismes de contrôle d'accès ont été introduits dans SSM pour fournir une amélioration de la sécurité non disponible avec les implémentations actuelles en mode clairsemé ou dense.

Limites :

- ASA ne peut pas servir de routeur de dernier saut pour la multidiffusion SSM, car il ne prend pas en charge IGMPv3 (que les destinataires utilisent pour joindre des groupes SSM).

  Si l'ASA est le dernier saut, il ignorera les messages de jonction IGMPv3 des destinataires pour les groupes SSM, et le transfert SSM ne fonctionnera pas.

- Les voies de routage de multidiffusion statiques sur ASA ne fonctionnent pas pour la plage SSM (232.x.x.x).

Solution de rechange:

Pour que le pare-feu Cisco ASA transfère le trafic de multidiffusion lié à SSM, vous devez ajouter un périphérique de couche 3 compatible avec la multidiffusion (comme un routeur ou un commutateur) qui prend en charge PIM et IGMPv3 sur le même segment de réseau que les récepteurs.

Modalités de fonctionnement :

- Les destinataires enregistrent leurs demandes d'adhésion aux groupes SSM (IGMPv3) auprès de ce périphérique de couche 3.
- Ce périphérique de couche 3 envoie des messages de jonction PIM vers l'ASA.
- L'ASA reçoit ces messages PIM et apprend dynamiquement les voies de routage de multidiffusion.
- Le trafic de multidiffusion SSM est ensuite correctement acheminé par l'ASA, car il ne s'agit plus du périphérique de dernier saut.

Routeur de démarrage PIM (BSR)

PIM Bootstrap Router (BSR) est un modèle de sélection dynamique des Points de Rendez vous (RP) qui utilise des routeurs candidats pour la fonction RP et pour le relais des informations RP pour un groupe.

La fonction RP comprend la découverte de RP et fournit une voie de routage par défaut vers le RP. Pour ce faire, elle configure un ensemble de périphériques en tant que candidats BSR (C-BSR) qui participent à un processus de sélection d'un BSR pour choisir un BSR parmi eux. Une fois le BSR choisi, les périphériques configurés en tant que points de rendez-vous candidats (C-RP) commencent à envoyer leur mappage de groupe au BSR élu. Le BSR distribue ensuite les informations de mappage groupe-RP à tous les autres périphériques en aval dans l'arborescence de multidiffusion par l'intermédiaire de messages du BSR qui voyagent de routeur PIM à routeur PIM par saut.

Cette fonctionnalité permet aux réseaux de découvrir dynamiquement les RP. La découverte dynamique des RP est essentielle dans les réseaux vastes et complexes où un RP peut occasionnellement tomber en panne puis redevenir opérationnel.

Terminologie du routeur de démarrage PIM (BSR)

Cette référence fournit des définitions des termes clés utilisés dans les configurations des routeurs de démarrage PIM (BSR) pour aider à comprendre les rôles et les fonctions des différents composants dans le processus d'élection de BSR et d'annonce de RP.

Les termes suivants sont fréquemment mentionnés dans la configuration du BSR PIM :

- Routeur Bootstrap (BSR) : un BSR annonce des informations de point de rendez-vous (RP) à d'autres routeurs avec PIM saut par saut. Parmi plusieurs candidats BSR, un seul BSR est choisi à l'issue d'un processus de sélection. L'objectif principal de ce routeur Bootstrap est de collecter toutes les annonces de Candidat RP (C-RP) dans une base de données appelée RP-set et de les envoyer périodiquement à tous les autres routeurs du réseau en tant que messages BSR (toutes les 60 secondes) .
- Messages Bootstrap Router (BSR) : les messages BSR sont en multidiffusion vers le groupe All-PIM-Routers avec une TTL de 1. Tous les voisins PIM qui reçoivent ces messages les retransmettent (encore une fois avec une TTL de 1) sur toutes les interfaces, à l'exception de celle dans laquelle les messages ont été reçus. Les messages BSR contiennent l'ensemble de RP et l'adresse IP du BSR actuellement actif. Voici comment les C-RP savent où envoyer en monodiffusion leurs messages C-RP.
- Candidate Bootstrap Router (C-BSR) : un appareil configuré en tant que candidat-BSR participe au mécanisme de sélection du BSR. Un C-BSR de priorité la plus élevée est choisi comme BSR. L'adresse IP la plus élevée de C-BSR est utilisée comme condition de départage. Le processus de sélection BSR est préemptif, par exemple, si un nouveau C-BSR avec une priorité plus élevée se présente, il déclenche un nouveau processus de sélection.
- Point de rendez-vous candidat (C-RP) : un RP sert de point de rencontre pour les sources et les récepteurs des données de multidiffusion. Un périphérique configuré en tant que C-RP annonce périodiquement les informations de mappage de groupe de multidiffusion directement au BSR choisi par la monodiffusion. Ces messages contiennent la plage de groupe, l'adresse C-RP et une durée d'attente. L'adresse IP du BSR actuel est apprise à partir des messages périodiques du BSR reçus par tous les routeurs du réseau. De cette façon, le BSR apprend quels sont les RP possibles qui sont actuellement actifs et accessibles.

Remarque L'ASA n'agit pas comme un C-RP, même si le C-RP est une exigence obligatoire pour le trafic BSR. Seuls les routeurs peuvent agir en tant que C-RP. Ainsi, pour la fonctionnalité de test du BSR, vous devez ajouter des routeurs à la topologie.

- Mécanisme de sélection BSR – Chaque C-BSR génère des messages Bootstrap (BSM) qui contiennent un champ de priorité BSR. Les routeurs du domaine inondent les BSM dans tout le domaine. Un C-BSR qui entend parler d'un C-BSR de priorité plus élevée que lui supprime l'envoi d'autres BSM pendant un certain temps. L'unique C-BSR restant devient le BSR élu, et ses BSM informent tous les autres routeurs du domaine qu'il est le BSR choisi.

Concept de groupe de multidiffusion

La multidiffusion est basée sur le concept de groupe. Un groupe arbitraire de récepteurs souhaite recevoir un flux de données particulier. Ce groupe n'a aucune limite physique ou géographique. Les hôtes peuvent être situés n'importe où sur Internet. Les hôtes qui souhaitent recevoir des données envoyées à un groupe doivent rejoindre le groupe à l'aide d'IGMP.

Exigences d'appartenance au groupe

Les hôtes doivent être membres du groupe pour recevoir le flux de données. Pour en savoir plus sur la configuration des groupes de multidiffusion, consultez Configurer un groupe de multidiffusion, à la page 1054.

Adresses de multidiffusion

Les adresses de multidiffusion spécifient un groupe quelconque d'hôtes IP qui ont rejoint le groupe et qui souhaitent recevoir le trafic envoyé à ce groupe.

Mise en grappe

Le routage de multidiffusion prend en charge la mise en grappe. Dans la mise en grappe étendue EtherChannel, l'unité de contrôle envoie tous les paquets de routage de multidiffusion et les paquets de données jusqu'à ce que le transfert rapide soit établi.

Une fois le transfert rapide établi, les unités de données peuvent transférer des paquets de données en multidiffusion. Tous les flux de données sont des flux complets. Les flux de transfert des tampons sont également pris en charge. Comme une seule unité reçoit les paquets en multidiffusion dans une grappe EtherChannel étendue, la redirection vers l'unité de contrôle est courante. Dans le regroupement d'interfaces individuelles, les unités n'agissent pas indépendamment. Toutes les données et les paquets de routage sont traités et transmis par l'unité de contrôle. Les unités de données abandonnent tous les paquets qui ont été envoyés.

Lignes directrices pour le routage de multidiffusion

Tableau 45 : Configuration système requise

Article	Description
Mode contextuel	Pris en charge en mode contexte unique
Mode pare-feu	Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.
IPv6	IPv6 n'est pas pris en charge.
Groupe de multidiffusion	La plage d'adresses entre 224.0.0.0 et 224.0.0.255 est réservée pour l'utilisation des protocoles de routage et d'autres protocoles de découverte ou de maintenance de topologie, tels que la découverte de passerelle et les rapports sur les membres de groupes. Le routage de multidiffusion Internet à partir de la plage d'adresses 224.0.0/24 n'est pas pris en charge. Lorsque le routage de multidiffusion est activé pour les adresses réservées, aucun groupe IGMP n'est créé.
Mise en grappes	En grappe, pour IGMP et PIM, cette fonctionnalité n'est prise en charge que sur l'unité principale.

Configuration du contrôle d'accès

Vous devez configurer une règle de contrôle d'accès sur l'interface entrante pour autoriser le trafic vers l'hôte de multidiffusion, comme l'interface 224.1.2.3. Cependant, vous ne pouvez pas spécifier une interface de destination pour la règle, ou elle ne peut pas être appliquée aux connexions en multidiffusion lors de la validation initiale de la connexion.

Gestion des interfaces et des protocoles

Assurez-vous d'une bonne gestion de la configuration lorsque vous utilisez des interfaces compatibles avec PIM et des protocoles de routage de multidiffusion.

- Le routage de multidiffusion n'est pas pris en charge dans ECMP.
- Ne configurez pas ASA pour être à la fois un point de rendez-vous (RP) et un routeur de premier saut.
- L'adresse IP de secours HSRP ne participe pas au voisinage PIM. Ainsi, si l'adresse IP du routeur PRV est acheminée par l'intermédiaire d'une adresse IP de secours HSRP, le routage de multidiffusion ne fonctionne pas dans ASA. Pour que le trafic en multidiffusion soit acheminé correctement, configurez la voie de routage vers l'adresse du PRV pour qu'elle utilise une adresse IP d'interface plutôt que l'adresse IP de secours HSRP.

Routage multidiffusion activé

L'activation du routage de multidiffusion sur l'ASA active l'IGMP et la PIM sur toutes les interfaces de données par défaut, mais pas sur l'interface de gestion pour la plupart des modèles (voir L'interface de logement/port de gestion, à la page 612 pour les interfaces qui n'autorisent pas le trafic). IGMP est utilisé pour savoir si les membres d'un groupe sont présents sur les sous-réseaux directement associés. Les hôtes se joignent aux groupes de multidiffusion en envoyant des messages de rapport IGMP. PIM est utilisé pour maintenir les tableaux de transfert pour transférer les datagrammes en multidiffusion.

Pour activer le routage de multidiffusion sur l'interface de gestion, vous devez définir explicitement une limite de multidiffusion sur l'interface de gestion.

Remarque Seule la couche de transport UDP est prise en charge pour le routage de multidiffusion.

La liste suivante indique le nombre maximal d'entrées pour des tableaux de multidiffusion spécifiques. Une fois ces limites atteintes, toute nouvelle entrée est rejetée.

- MFIB : 30 000
- Groupes IGMP : 30 000
- Routages PIM : 72 000

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)**.

Étape 2 Dans le volet Multicast (Multidiffusion), cochez la case **Enable Multicast routing** (Activer le routage de multidiffusion).

Cochez cette case pour activer le routage de multidiffusion IP sur l'ASA. Décocher cette case désactive le routage de multidiffusion IP. Par défaut, la multidiffusion est désactivée. L'activation du routage de multidiffusion active la multidiffusion sur toutes les interfaces. Vous pouvez désactiver la multidiffusion interface par interface.

Personnaliser le routage multidiffusion

Cette section décrit comment personnaliser le routage multidiffusion.

Configurer le routage de multidiffusion Stub et transférer les messages IGMP



Remarque Le routage de multidiffusion de stub n'est pas pris en charge en même temps que les modes fragmenté et bidirectionnel de la PIM.

Un ASA agissant en tant que passerelle vers la zone de stub n'a pas besoin de participer au mode fractionné (PIM) ou au mode bidirectionnel. Au lieu de cela, vous pouvez le configurer pour qu'il agisse comme un agent mandataire et transfère les messages IGMP des hôtes connectés sur une interface vers un routeur de multidiffusion en amont sur une autre interface. Pour configurer l'ASA en tant qu'agent de mandataire IGMP, transférez les messages de jonction et de sortie de l'hôte de l'interface de zone de stub vers une interface en amont. Vous devez également activer la PIM sur les interfaces qui participent au routage de multidiffusion en mode stub.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)**.

Étape 2 Dans le volet Multicast (Multidiffusion), cochez la case **Enable Multicast routing** (Activer le routage de multidiffusion).

Étape 3 Cliquez sur **Apply** pour enregistrer vos modifications.

Étape 4 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Protocol (Protocole)**.

Étape 5 Pour modifier l'interface à partir de laquelle vous souhaitez transférer les messages IGMP, sélectionnez l'interface et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Configure IGMP Parameters** (Configurer les paramètres IGMP) apparaît.

Étape 6 Dans la liste déroulante **Forward Interface** (Interface de transfert), choisissez l'interface spécifique à partir de laquelle vous souhaitez transférer les messages IGMP.

Étape 7 Cliquez sur **OK** pour fermer cette boîte de dialogue, puis cliquez sur **Apply** (Appliquer) pour enregistrer vos modifications.

Configurer une route de multidiffusion statique

La configuration de routes statiques de multidiffusion vous permet de séparer le trafic de multidiffusion du trafic de monodiffusion. Par exemple, quand un chemin entre une source et une destination ne prend pas en charge le routage de multidiffusion, la solution consiste à configurer deux périphériques de multidiffusion avec un tunnel GRE et d'envoyer les paquets en multidiffusion sur le tunnel.

Lors de l'utilisation de PIM, l'ASA s'attend à recevoir des paquets sur la même interface où il renvoie les paquets de monodiffusion à la source. Dans certains cas, par exemple pour contourner une voie de routage qui ne prend pas en charge le routage de multidiffusion, vous pouvez souhaiter que les paquets monodiffusion prennent un chemin et les paquets multidiffusion, un autre.

Les routes de multidiffusion statiques ne sont pas annoncées ou redistribuées.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **MRoute**.

Étape 2 Choisissez **Add** (Ajouter) ou **Edit** (Modifier).

La boîte de dialogue Add or Edit Multicast Route (Ajouter ou modifier une route de multidiffusion) s'affiche.

Utilisez la boîte de dialogue Add Multicast Route (Ajouter une route de multidiffusion) pour ajouter une nouvelle route de multidiffusion statique à l'ASA. Utilisez la boîte de dialogue Edit Multicast Route (Modifier une route de multidiffusion) pour modifier une route de multidiffusion statique existante.

Étape 3 Dans le champ Source Address (Adresse source), saisissez l'adresse IP de la source de multidiffusion. Vous ne pouvez pas modifier cette valeur lors de la modification d'une route de multidiffusion statique existante.

Étape 4 Choisissez le masque réseau pour l'adresse IP de la source de multidiffusion dans la liste déroulante Source Mask (Masque source).

Étape 5 Dans la zone Incoming Interface (Interface entrante), cliquez sur le bouton radio **RPF Interface** (Interface RPF) pour choisir RPF pour transférer le routage ou sur le bouton radio **Interface Name** (Nom de l'interface), puis saisissez la commande suivante :

- Dans le champ Source Interface (Interface source), choisissez l'interface entrante pour la route de multidiffusion dans la liste déroulante.
- Dans le champ Destination Interface (Interface de destination), choisissez l'interface de destination par laquelle la route est transférée dans la liste déroulante.

Remarque Vous pouvez spécifier l'interface ou le voisin RPF, mais pas les deux en même temps.

Étape 6 Dans le champ Administrative Distance (Distance administrative), choisissez la distance administrative de la route de multidiffusion statique. Si la route de multidiffusion statique a la même distance administrative que la route de monodiffusion, la route de multidiffusion statique prévaut.

Étape 7 Cliquez sur **OK**.

Configurer des fonctionnalités IGMP

Les hôtes IP utilisent le protocole IGMP pour signaler leur appartenance à des groupes aux routeurs de multidiffusion connectés directement. IGMP est utilisé pour enregistrer dynamiquement des hôtes individuels dans un groupe de multidiffusion sur un réseau local particulier. Les hôtes déterminent les appartenances aux groupes en envoyant des messages IGMP à leur routeur de multidiffusion local. Sous IGMP, les routeurs écoutent les messages IGMP et envoient périodiquement des requêtes pour découvrir quels groupes sont actifs ou inactifs sur un sous-réseau particulier.

Cette section décrit comment configurer les paramètres IGMP facultatifs pour l'interface.

Désactiver IGMP sur une interface

Vous pouvez désactiver IGMP sur des interfaces spécifiques. Cela est utile si vous savez qu'il n'y a aucun hôte en multidiffusion sur une interface spécifique et que vous souhaitez empêcher l'ASA d'envoyer des messages de requête d'hôte sur cette interface.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Protocol (Protocole)**.

Le volet Protocol (Protocole) affiche les paramètres IGMP pour chaque interface de l'ASA.

Étape 2 Sélectionnez l'interface que vous souhaitez désactiver et cliquez sur **Edit** (Modifier).

Étape 3 Pour désactiver l'interface spécifiée, décochez la case **Enable IGMP** (Activer IGMP).

Étape 4 Cliquez sur **OK**.

Le volet Protocol (Protocole) affiche Yes (Oui) si IGMP est activé sur l'interface ou No (Non) si IGMP est désactivé sur l'interface.

Configurer l'appartenance au groupe IGMP

Vous pouvez configurer l'ASA pour qu'il soit membre d'un groupe de multidiffusion. La configuration de l'ASA pour se joindre à un groupe de multidiffusion fait en sorte que les routeurs en amont conservent les renseignements de la table de routage de multidiffusion pour ce groupe et maintiennent les chemins de ce groupe actifs.

Remarque Si vous souhaitez transférer des paquets en multidiffusion pour un groupe spécifique vers une interface sans que l'ASA n'accepte ces paquets dans le cadre du groupe, consultez Configurer un groupe IGMP joint statiquement, à la page 1046.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Join Group (Groupe de jonction)**.

Étape 2 Cliquez sur **Add** (Ajouter) ou **Edit** > **(Modifier) dans le volet** > **Join Group** > **(Groupe de jonction)**.

La boîte de dialogue Add IGMP Join Group (Ajouter un groupe de jonction IGMP) vous permet de configurer une interface pour qu'elle soit membre d'un groupe de multidiffusion. La boîte de dialogue Edit IGMP Join Group (Modifier un groupe de jonction IGMP) vous permet de modifier les renseignements d'appartenance existants.

Étape 3 Dans le champ Interface Name (Nom de l'interface), choisissez le nom de l'interface dans la liste déroulante. Si vous modifiez une entrée existante, vous ne pouvez pas modifier cette valeur.

Étape 4 Dans le champ Multicast Group Address (Adresse de groupe de multidiffusion), saisissez l'adresse d'un groupe de multidiffusion auquel appartient l'interface. Les adresses de groupe valides sont comprises entre 224.0.0.0 et 239.255.255.255.

Étape 5 Cliquez sur **OK**.

Configurer un groupe IGMP joint statiquement

Parfois, un membre d'un groupe ne peut pas signaler son appartenance au groupe en raison d'une configuration, ou il se peut qu'il n'y ait aucun membre d'un groupe sur le segment de réseau. Cependant, vous souhaitez toujours que le trafic de multidiffusion de ce groupe soit envoyé vers ce segment de réseau. Vous pouvez envoyer le trafic de multidiffusion pour ce groupe au segment en configurant un groupe IGMP rejoint statiquement.

Dans la fenêtre principale d'ASDM, choisissez **Configuration > Routing (Routage) > Multicast (Multidiffusion) > IGMP > Static Group (Groupe statique)** pour configurer l'ASA en tant que membre connecté de manière statique à un groupe. Avec cette méthode, l'ASA n'accepte pas les paquets lui-même, mais les transfère seulement. Par conséquent, cette méthode permet une commutation rapide. L'interface sortante apparaît dans le cache IGMP, mais cette interface n'est pas membre du groupe de multidiffusion.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Static Group (Groupe statique)**.

Étape 2 Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans le volet **Static Group** (Groupe statique).

Utilisez la boîte de dialogue Add IGMP Static Group (Ajouter un groupe statique IGMP) pour affecter de manière statique un groupe de multidiffusion à une interface. Utilisez la boîte de dialogue Edit IGMP Static Group (Modifier un groupe statique IGMP) pour modifier les affectations de groupes statiques existantes.

Étape 3 Dans le champ Interface Name (Nom de l'interface), choisissez le nom de l'interface dans la liste déroulante. Si vous modifiez une entrée existante, vous ne pouvez pas modifier cette valeur.

Étape 4 Dans le champ Multicast Group Address (Adresse de groupe de multidiffusion), saisissez l'adresse d'un groupe de multidiffusion auquel appartient l'interface. Les adresses de groupe valides sont comprises entre 224.0.0.0 et 239.255.255.255.

Étape 5 Cliquez sur **OK**.

Contrôler l'accès aux groupes de multidiffusion

Vous pouvez contrôler l'accès aux groupes de multidiffusion à l'aide de listes de contrôle d'accès.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Access Group (Groupe d'accès)**.

Le volet Access Group (Groupe d'accès) apparaît. Les entrées du tableau dans le volet Access Group (Groupe d'accès) sont traitées de haut en bas. Placez les entrées plus spécifiques en haut du tableau et les entrées plus génériques plus bas. Par exemple, placez une entrée de groupe d'accès qui autorise un groupe de multidiffusion spécifique près du haut du tableau et une entrée de groupe d'accès en dessous qui refuse une plage de groupes de multidiffusion, y compris le groupe dans la règle d'autorisation. Le groupe est autorisé car la règle d'autorisation est appliquée avant la règle de refus.

Un double-clic sur une entrée du tableau ouvre la boîte de dialogue Add or Edit Access Group (Ajouter ou modifier un groupe d'accès) pour l'entrée sélectionnée.

Étape 2 Cliquez sur **Add** ou **Edit** (ajouter ou modifier).

La boîte de dialogue Add Access Group (Ajouter un groupe d'accès) ou Edit Access Group (Modifier un groupe d'accès) apparaît. La boîte de dialogue Add Access Group (Ajouter un groupe d'accès) vous permet d'ajouter un nouveau groupe d'accès au tableau des groupes d'accès. La boîte de dialogue Edit Access Group (Modifier un groupe d'accès) vous permet de modifier les renseignements d'une entrée de groupe d'accès existante. Certains champs peuvent être grisés lors de la modification des entrées existantes.

Étape 3 Choisissez le nom d'interface auquel le groupe d'accès est associé dans la liste déroulante Interface. Vous ne pouvez pas modifier l'interface associée lorsque vous modifiez un groupe d'accès existant.

Étape 4 Choisissez permit (autoriser) dans la liste déroulante Action pour autoriser le groupe de multidiffusion sur l'interface sélectionnée. Choisissez deny (refuser) dans la liste déroulante Action pour filtrer le groupe de multidiffusion de l'interface sélectionnée.

Étape 5 Dans le champ Multicast Group Address (Adresse de groupe de multidiffusion), saisissez l'adresse du groupe de multidiffusion auquel le groupe d'accès s'applique.

Étape 6 Saisissez le masque réseau pour l'adresse du groupe de multidiffusion ou sélectionnez l'un des masques réseau courants dans la liste déroulante Netmask (Masque réseau).

Étape 7 Cliquez sur **OK**.

Limiter le nombre d'états IGMP sur une interface

Vous pouvez limiter le nombre d'états IGMP résultant des rapports sur les membres IGMP pour chaque interface. Les rapports sur les membres dépassant les limites configurées ne sont pas entrés dans la mémoire cache IGMP et le trafic pour les rapports sur les membres excédentaires n'est pas transféré.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface que vous souhaitez limiter dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Configure IGMP Parameters (Configurer les paramètres IGMP) apparaît.

Étape 3 Dans le champ Group Limit (Limite de groupe), saisissez le nombre maximum d'hôtes qui peuvent rejoindre une interface.

La valeur par défaut est 500. Les valeurs valides sont comprises entre 0 et 5 000.

Remarque La définition de cette valeur à 0 empêche l'ajout de groupes appris, mais les appartenances définies manuellement sont toujours autorisées.

Étape 4 Cliquez sur **OK**.

Remarque Lorsque vous modifiez la limite IGMP sur l'interface avec des jonctions actives, la nouvelle limite ne s'applique pas aux groupes existants. L'ASA valide la limite uniquement lorsqu'un nouveau groupe est ajouté à l'interface ou lorsque les minuteries de jonction IGMP expirent. Pour appliquer la nouvelle limite avec effet immédiat, vous devez désactiver et réactiver IGMP sur l'interface.

Modifier les messages de requête destinés aux groupes de multidiffusion

L'ASA envoie des messages de requête pour découvrir quels groupes de multidiffusion ont des membres sur les réseaux connectés aux interfaces. Les membres répondent par des messages de rapport IGMP indiquant qu'ils souhaitent recevoir des paquets en multidiffusion pour des groupes spécifiques. Les messages de requête sont adressés au groupe de multidiffusion tous les systèmes, qui possède l'adresse 224.0.0.1 et une valeur de durée de vie de 1.

Ces messages sont envoyés périodiquement pour actualiser les renseignements sur les membres stockés sur l'ASA. Si l'ASA découvre qu'il n'y a aucun membre local d'un groupe de multidiffusion connecté à une

interface, il arrête de transférer le paquet en multidiffusion pour ce groupe vers le réseau connecté et il renvoie un message d'élaguer à la source des paquets.

Par défaut, le routeur désigné PIM sur le sous-réseau est responsable de l'envoi des messages de requête. Par défaut, ils sont envoyés toutes les 125 secondes.

Lors de la modification du temps de réponse aux requêtes, par défaut, le temps de réponse maximal aux requêtes annoncé dans les requêtes IGMP est de 10 secondes. Si l'ASA ne reçoit pas de réponse à une requête d'hôte dans ce délai, il supprime le groupe.

Pour modifier l'intervalle de requête, le temps de réponse à la requête et la valeur du délai d'expiration de la requête, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface que vous souhaitez limiter dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Configure IGMP Parameters (Configurer les paramètres IGMP) apparaît.

Étape 3 Dans le champ **Query Interval** (Intervalle de requête), saisissez l'intervalle en secondes auquel le routeur désigné envoie des messages de requête d'hôte IGMP.

Les valeurs valides vont de 1 à 3 600 secondes. La valeur par défaut est 125 secondes.

Remarque Si l'ASA n'entend pas de message de requête sur une interface pendant le délai d'expiration spécifié, l'ASA devient le routeur désigné et commence à envoyer les messages de requête.

Étape 4 Dans le champ **Query Timeout** (Délai d'expiration de la requête), saisissez la période en secondes avant laquelle l'ASA prend le relais en tant que demandeur pour l'interface après l'arrêt du demandeur précédent.

Les valeurs valides vont de 60 à 300 secondes. La valeur par défaut est 255secondes.

Étape 5 Dans le champ **Response Time** (Temps de réponse), saisissez le temps de réponse maximum annoncé dans les requêtes IGMP, en secondes.

Les valeurs sont comprises entre 1 et 25 secondes. La valeur par défaut est 10 secondes.

Étape 6 Cliquez sur **OK**.

Modifier la version IGMP

Par défaut, l'ASA exécute la version 2 du protocole IGMP, qui active plusieurs fonctionnalités supplémentaires.

Tous les routeurs de multidiffusion d'un sous-réseau doivent prendre en charge la même version d'IGMP. L'ASA ne détecte pas automatiquement les routeurs de la version 1 et passe à la version 1. Cependant, une combinaison d'hôtes IGMP versions 1 et 2 sur le sous-réseau fonctionne; l'ASA exécutant IGMP version 2 fonctionne correctement lorsque des hôtes IGMP version 1 sont présents.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface dont vous souhaitez modifier la version d'IGMP dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Configure IGMP Interface (Configurer l'interface IGMP) apparaît.

Étape 3 Choisissez le numéro de version dans la liste déroulante Version.

Étape 4 Cliquez sur **OK**.

Configurer des fonctionnalités PIM

Les routeurs utilisent PIM pour gérer les tableaux de transfert à utiliser pour le transfert des diagrammes de multidiffusion. Lorsque vous activez le routage de multidiffusion sur ASA, PIM et IGMP sont automatiquement activés sur toutes les interfaces.



Remarque Le protocole PIM n'est pas pris en charge avec PAT. Le protocole PIM n'utilise pas de ports et PAT ne fonctionne qu'avec les protocoles qui utilisent des ports.

Cette section décrit comment configurer les paramètres PIM optionnels.

Activer et désactiver la PIM sur une interface

Vous pouvez activer ou désactiver la PIM sur des interfaces spécifiques.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface sur laquelle vous souhaitez activer la PIM dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit PIM Protocol** (Modifier le protocole PIM) apparaît.

Étape 3 Cochez la case **Enable PIM** (Activer la PIM). Pour désactiver la PIM, décochez cette case.

Étape 4 Cliquez sur **OK**.

Configurer une adresse de point de rendez-vous statique

Tous les routeurs d'un mode PIM fragmenté ou d'un domaine bidirectionnel commun doivent connaître l'adresse PRV PIM. L'adresse est configurée de manière statique à l'aide de la commande **pim rp-address**.

Remarque L'ASA ne prend pas en charge le PRV automatique.

Vous pouvez configurer l'ASA pour qu'il serve de PRV à plus d'un groupe. La plage de groupes spécifiée dans la liste de contrôle d'accès détermine le mappage du groupe RP PIM. Si aucune ACL n'est précisée, le RP du groupe est appliqué à l'ensemble de la plage du groupe de multidiffusion (224.0.0.0/4).

Procédure

Étape 1 Dans la fenêtre principale ASDM, choisissez**Configuration** > **Configuration du périphérique** > **Routage** > **Multidiffusion** > **PIM** > **Points de rendezvous**.

Étape 2 Cliquez sur **Add** ou **Edit** (Ajouter ou modifier).

La boîte de dialogue Add or Edit Rendezvous Point (Ajouter ou modifier un point de rendez-vous) s'affiche. La boîte de dialogue **Add Rendezvous Point** (Ajouter un point de rendez-vous) vous permet d'ajouter une nouvelle entrée au tableau des points de rendez-vous. La boîte de dialogue Edit Rendezvous Point (Modifier un point de rendez-vous) vous permet de modifier une entrée PRV existante. En outre, vous pouvez cliquer sur **Delete** (Supprimer) pour supprimer l'entrée du groupe de multidiffusion sélectionnée du tableau.

Ces restrictions s'appliquent aux PRV :

- Vous ne pouvez pas utiliser deux fois la même adresse RP.
- Vous ne pouvez pas spécifier Tous les groupes pour plus d'un RP.

Étape 3 Dans le champ **Rendezvous Point Address** (Adresse du point de rendez-vous), saisissez l'adresse IP du point de rendez-vous (PRV).

Lorsque vous modifiez une entrée PRV existante, vous ne pouvez pas modifier cette valeur.

Étape 4 Cochez la case **Use bi-directionnel forwarding** (Utiliser le transfert bidirectionnel) si les groupes de multidiffusion spécifiés doivent fonctionner en mode bidirectionnel. Le volet Rendezvous Point (Point de rendez-vous) affiche Yes (Oui) si les groupes de multidiffusion spécifiés doivent fonctionner en mode bidirectionnel et No (Non) si ces groupes doivent fonctionner en mode fragmenté. En mode bidirectionnel, si l'ASA reçoit un paquet en multidiffusion et n'a aucun membre connecté directement ou voisin PIM présent, il renvoie un message de suppression à la source.

Étape 5 Cliquez sur le bouton radio **Use this RP for All Multicast Groups** (Utiliser ce PRV pour tous les groupes de multidiffusion) pour utiliser le PRV spécifié pour tous les groupes de multidiffusion sur l'interface, ou sur le bouton radio **Use this RP for the Multicast Groups as specified below** (Utiliser ce PRV pour les groupes de multidiffusion spécifiés ci-dessous) pour désigner les groupes de multidiffusion à utiliser avec le PRV spécifié.

Pour en savoir plus sur les groupes de multidiffusion, consultez Configurer un groupe de multidiffusion, à la page 1054.

Étape 6 Cliquez sur **OK**.

Configurer la priorité des routeurs désignés

Le DR est responsable de l'envoi des messages PIM de registre, de jonction et de suppression au RP. Lorsqu'il y a plusieurs routeurs de multidiffusion sur un segment de réseau, la sélection du DR se fait en fonction de la priorité DR. Si plusieurs périphériques ont le même DR, le périphérique avec l'adresse IP la plus élevée devient DR.

Par défaut, l'ASA a une priorité DR de 1. Vous pouvez modifier cette valeur.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface que vous souhaitez activer pour la PIM dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Edit PIM Protocol (Modifier le protocole PIM) apparaît.

Étape 3 Dans le champ DR Priority (Priorité DR), saisissez la valeur de la priorité de routeur désigné pour l'interface sélectionnée. Le routeur ayant la priorité DR la plus élevée sur le sous-réseau devient le routeur désigné. Les valeurs valides sont comprises entre 0 et 4294967294. La priorité DR par défaut est 1. Si cette valeur est fixée à 0, l'interface de l'ASA ne peut pas devenir le routeur par défaut.

Étape 4 Cliquez sur **OK**.

Configurer et filtrer les messages de registre PIM

Lorsque l'ASA agit comme un PRV, vous pouvez empêcher certaines sources en multidiffusion de s'enregistrer auprès de lui pour empêcher les sources non autorisées de s'enregistrer auprès du PRV. Le volet Request Filter (Filtre de demande) vous permet de définir les sources en multidiffusion dont l'ASA accepte les messages de registre PIM.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Request Filter (Filtre de demande)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue Request Filter Entry (Entrée du filtre de demande) vous permet de définir les sources de multidiffusion qui sont autorisées à s'enregistrer auprès de l'ASA lorsque celui-ci agit en tant que PRV. Vous créez les règles de filtre en fonction de l'adresse IP source et de l'adresse de multidiffusion de destination.

Étape 3 Dans la liste déroulante Action, sélectionnez Permet (Autoriser) pour créer une règle qui autorise la source spécifiée du trafic de multidiffusion spécifié à s'enregistrer auprès de l'ASA, ou sélectionnez Deny (Refuser)

pour créer une règle qui empêche la source spécifiée du trafic de multidiffusion spécifié de s'enregistrer auprès de l'ASA.

Étape 4 Saisissez l'adresse IP de la source du message de registre dans le champ Source IP Address (Adresse IP source).

Étape 5 Saisissez ou choisissez le masque réseau dans la liste déroulante de la source du message de registre, dans le champ Source Netmask (Masque réseau source).

Étape 6 Saisissez l'adresse de multidiffusion de destination dans le champ Destination IP Address (Adresse IP de destination).

Étape 7 Saisissez ou choisissez le masque réseau dans la liste déroulante de l'adresse de multidiffusion de destination, dans le champ Destination Netmask (Masque réseau de destination).

Étape 8 Cliquez sur **OK**.

Configurer les intervalles des messages PIM

Les messages de requête de routeur sont utilisés pour sélectionner le PIM DR. Le PIM DR est responsable de l'envoi des messages d'interrogation du routeur. Par défaut, des messages de requête du routeur sont envoyés toutes les 30 secondes. En outre, toutes les 60 secondes, l'ASA envoie des messages de jonction ou d'élimination PIM.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Protocol (Protocole)**.

Étape 2 Choisissez l'interface que vous souhaitez activer pour la PIM dans le tableau du volet Protocol (Protocole), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Edit PIM Protocol (Modifier le protocole PIM) apparaît.

Étape 3 Saisissez la fréquence, en secondes, à laquelle l'interface envoie des messages Hello PIM, dans le champ Hello Interval (Intervalle Hello).

Étape 4 Saisissez la fréquence, en secondes, à laquelle l'interface envoie des annonces de jonction et d'élimination PIM, dans le champ Prune Interval (Intervalle d'élimination).

Étape 5 Cliquez sur **OK**.

Configurer une arborescence de routes

Par défaut, les routeurs secondaires PIM rejoignent l'arborescence du chemin le plus court immédiatement après l'arrivée du premier paquet en provenance d'une nouvelle source. Cette méthode réduit les délais, mais nécessite plus de mémoire que l'arborescence partagée. Vous pouvez configurer si l'ASA doit se joindre à l'arborescence du chemin le plus court ou utiliser l'arborescence partagée, soit pour tous les groupes de multidiffusion, soit uniquement pour des adresses de multidiffusion spécifiques.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Route Tree (Arborescence des routes)**.

Étape 2 Cliquez sur l'un des boutons radio suivants :

- **Use Shortest Path Tree for All Groups** (Utiliser l'arborescence du chemin le plus court pour tous les groupes) : choisissez cette option pour utiliser l'arborescence du chemin le plus court pour tous les groupes de multidiffusion.
- **Use Shared Tree for All Groups** (Utiliser l'arborescence partagée pour tous les groupes) pour utiliser l'arborescence partagée pour tous les groupes de multidiffusion.
- **Use Shared Tree for the Groups specified below** (Utiliser l'arborescence partagée pour les groupes spécifiés ci-dessous) : choisissez cette option pour utiliser l'arborescence partagée pour les groupes spécifiés dans le tableau des groupes de multidiffusion. L'arborescence du chemin le plus court est utilisée pour tout groupe qui n'est pas spécifié dans le tableau Groupes de multidiffusion.

  Le tableau Groupes de multidiffusion affiche les groupes de multidiffusion à utiliser avec l'arborescence partagée.

  Les entrées du tableau sont traitées de haut en bas. Vous pouvez créer une entrée qui comprend une plage de groupes de multidiffusion, mais exclut des groupes spécifiques de cette plage en mettant des règles de refus pour les groupes spécifiques en haut du tableau et la règle d'autorisation pour la plage de groupes en multidiffusion en dessous des instructions de refus.

  Pour modifier un groupe de multidiffusion, consultez Configurer un groupe de multidiffusion, à la page 1054.

Configurer un groupe de multidiffusion

Les groupes de multidiffusion sont des listes de règles d'accès qui définissent les adresses de multidiffusion qui font partie d'un groupe. Un groupe de multidiffusion peut comprendre une adresse de multidiffusion unique ou une plage d'adresses de multidiffusion. Utilisez la boîte de dialogue Add Multidiffusion Group (Ajouter un groupe de multidiffusion) pour créer une nouvelle règle de groupe de multidiffusion. Utilisez la boîte de dialogue Edit Multicast Group (Modifier un groupe de multidiffusion) pour modifier une règle de groupe de multidiffusion existante.

Pour configurer un groupe de multidiffusion, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale ASDM, choisissez**Configuration** > **Configuration du périphérique** > **Routage** > **Multidiffusion** > **PIM** > **Points de rendezvous**.

Étape 2 Le volet Rendezvous Point s'affiche. Cliquez pour enregistrer le groupe que vous souhaitez configurer.

La boîte de dialogue Edit Rendezvous Point (Modifier le point de rendez-vous) s'affiche.

Étape 3 Cliquez sur le bouton d' **option Use this RP for the Multicast Groups comme précisé sous** le bouton radio pour désigner les groupes de multidiffusion à utiliser avec le RP précisé.

Étape 4 Cliquez sur **Add** ou **Edit**(ajouter ou modifier) .

La boîte de dialogue Add or Edit Multicast Group (ajouter ou modifier un groupe de multidiffusion) s'affiche.

Étape 5 Dans la liste déroulante Action (action), choisissez Allow pour créer une règle de groupe qui autorise les adresses de multidiffusion précisées ou choisissez Deny (refuser) pour créer une règle de groupe qui filtre les adresses de multidiffusion précisées.

Étape 6 Dans le champ Multicast Group Address (adresse de groupe de multidiffusion), saisissez l'adresse de multidiffusion associée au groupe.

Étape 7 Dans la liste déroulante Netmask, choisissez le masque de réseau pour l'adresse de groupe de multidiffusion.

Étape 8 Cliquez sur **OK**.

Filtrer les voisins PIM

Vous pouvez définir les routeurs qui peuvent devenir des voisins PIM. En filtrant les routeurs qui peuvent devenir des voisins PIM, vous pouvez effectuer les opérations suivantes :

- Empêchez les routeurs non autorisés de devenir des voisins PIM.
- Empêchez les routeurs tampons connectés de participer à PIM.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Neighbor Filter (Filtre de voisin)**.

Étape 2 Choisissez le voisin PIM que vous souhaitez configurer dans le tableau en cliquant sur **Add** (Ajouter)/**Edit** (Modifier)/**Insert** (Insérer).

La boîte de dialogue **Add/Edit/Insert Neighbor Filter Entry** (Ajouter/modifier/insérer une entrée de filtre de voisin) s'affiche. Elle vous permet de créer les entrées ACL pour la liste de contrôle d'accès de limite de multidiffusion. Vous pouvez également supprimer une entrée de voisin PIM sélectionnée.

Étape 3 Choisissez le nom de l'interface dans la liste déroulante **Interface Name** (Nom de l'interface).

Étape 4 Dans la liste déroulante **Action**, choisissez **Permit** (Autoriser) ou **Deny** (Refuser) pour l'entrée ACL du filtre de voisin.

Choisir Permit (Autoriser) permet aux annonces de groupes de multidiffusion de passer par l'interface. Si vous choisissez Deny (Refuser), les annonces de groupe de multidiffusion précisées ne passent pas par l'interface. Lorsqu'une limite de multidiffusion est configurée sur une interface, tout le trafic en multidiffusion ne peut pas passer par l'interface, à moins qu'une entrée de filtre de voisin ne le permette.

Étape 5 Saisissez l'adresse IP du groupe de PIM de multidiffusion autorisé ou refusé dans le champ **IP Address** (Adresse IP). Les adresses de groupe valides sont comprises entre 224.0.0.0 et 239.255.255.255.

Étape 6 Dans la liste déroulante **Netmask** (Masque réseau), choisissez le masque réseau pour l'adresse de groupe de multidiffusion.

Étape 7 Cliquez sur **OK**.

Configurer un filtre de voisin bidirectionnel PIM

Le volet Bidirectional Neighbor Filter (Filtre de voisin bidirectionnel) affiche les filtres de voisin bidirectionnel de la PIM, le cas échéant, qui sont configurés sur l'ASA. Un filtre de voisin bidirectionnel PIM est une ACL qui définit les périphériques voisins pouvant participer au choix du DF. Si un filtre de voisin bidirectionnel PIM n'est pas configuré pour une interface, il n'y a aucune restriction. Si un filtre de voisin bidirectionnel PIM est configuré, seuls les voisins autorisés par la liste de contrôle d'accès peuvent participer au processus de sélection de DF.

Lorsqu'une configuration de filtre de voisin bidirectionnel PIM est appliquée à l'ASA, une ACL s'affiche dans la configuration en cours d'exécution avec le nom *interface-name_multicast*, dans lequel le *interface-name* est le nom de l'interface à laquelle le filtre de limite de multidiffusion est appliqué. Si une ACL porte déjà ce nom, un numéro est affecté au nom (par exemple, inside_multicast_1). Cette ACL définit quels appareils peuvent devenir des voisins PIM de l'ASA.

Le PIM bidirectionnel permet aux routeurs de multidiffusion de conserver des informations d'état réduites. Tous les routeurs de multidiffusion d'un segment doivent être activés de manière bidirectionnelle pour choisir un DF.

Les filtres de voisin bidirectionnels de la PIM permettent la transition d'un réseau en mode fragmenté uniquement vers un réseau bidirectionnel en vous permettant de spécifier les routeurs qui doivent participer au choix du DF, tout en permettant à tous les routeurs de participer au domaine en mode fragmenté. Les routeurs bidirectionnels peuvent choisir un DF entre eux, même s'il y a des routeurs non-bidirectionnels sur le segment. La multidiffusion sur les routeurs non-bidirectionnels empêche les messages PIM et les données des groupes bidirectionnels de fuir vers l'intérieur ou l'extérieur du sous-ensemble bidirectionnel.

Lorsqu'un filtre de voisin bidirectionnel PIM est activé, les routeurs autorisés par la liste de contrôle d'accès sont considérés comme bidirectionnels. Par conséquent, ce qui suit est vrai :

- Si un voisin autorisé ne prend pas en charge le mode bidirectionnel, le choix du DF n'a pas lieu.
- Si un voisin refusé prend en charge le mode bidirectionnel, le choix du DF n'a pas lieu.
- Si un voisin refusé ne prend pas en charge le mode bidirectionnel, le choix du DF peut avoir lieu.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration du périphérique)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Bidirectional Neighbor Filter (Filtre de voisin bidirectionnel)**.

Étape 2 Cliquez deux fois sur une entrée dans le tableau des filtres de voisins bidirectionnels PIM pour accéder à la boîte de dialogue Edit Bidirectional Neighbor Filter Entry (Modifier une entrée de filtre de voisin bidirectionnel) pour cette entrée.

Étape 3 Choisissez le voisin PIM que vous souhaitez configurer dans le tableau en cliquant sur **Add** (Ajouter)/**Edit** (Modifier)/**Insert** (Insérer).

La boîte de dialogue **Add/Edit/Insert Bidirectional Neighbor Filter Entry (Ajouter/Modifier/Insérer une entrée de filtre de voisin bidirectionnel)** apparaît pour créer des entrées ACL pour l'ACL du filtre de voisin bidirectionnel PIM.

Étape 4 Choisissez le nom de l'interface dans la liste déroulante **Interface Name** (Nom de l'interface). Sélectionnez l'interface pour laquelle vous souhaitez configurer l'entrée ACL du filtre de voisin bidirectionnel PIM.

Étape 5 Dans la liste déroulante **Action**, choisissez **Permit** (Autoriser) ou **Deny** (Refuser) pour l'entrée ACL du filtre de voisin.

Choisissez Permit (Autoriser) pour autoriser les périphériques spécifiés à participer au processus de sélection du DF. Choisissez Deny (Refuser) pour empêcher les périphériques spécifiés de participer au processus de sélection du DF.

Étape 6 Saisissez l'adresse IP du groupe PIM de multidiffusion qui est autorisé ou refusé. Les adresses de groupe valides sont comprises entre 224.0.0.0 et 239.255.255.255, dans le champ IP Address (Adresse IP).

Étape 7 Dans la liste déroulante Netmask (Masque réseau), choisissez le masque réseau pour l'adresse de groupe de multidiffusion.

Étape 8 Cliquez sur **OK**.

Configurer l'ASA comme candidat BSR

Vous pouvez configurer l'ASA en tant que BSR candidat. Cela facilite également la découverte automatique du point de rendez-vous (PRV).

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **PIM** > **Bootstrap Router (Routeur de démarrage)**.

Étape 2 Cochez la case **Configure this ASA as a candidate bootstrap router (CBSR)** (Configurer cet ASA en tant que routeur de démarrage candidat (CBSR)) pour effectuer la configuration de CBSR.

a) Dans la liste déroulante **Select Interface** (Sélectionner l'interface), sélectionnez l'interface sur l'ASA dont l'adresse BSR est dérivée pour en faire une interface candidate.

Remarque Cette interface doit être activée avec PIM.

b) Dans le champ **Hash mask length** (Longueur du masque de hachage), saisissez la longueur du masque (32 bits maximum) qui doit faire l'objet d'un AND avec l'adresse de groupe avant que la fonction de hachage ne soit appelée. Tous les groupes ayant le même hachage de départ correspondent au même point de rendez-vous (PRV). Par exemple, si cette valeur est 24, seuls les 24 premiers bits des adresses de groupe importent. Ce fait vous permet d'obtenir un RP pour plusieurs groupes.

c) Saisissez la priorité du BSR candidat dans le champ **Priority** (Priorité). Le BSR ayant la plus grande priorité est privilégié. Si les valeurs de priorité sont les mêmes, le routeur avec la plus grande adresse IP est le BSR. La valeur par défaut est 0.

Étape 3 (Facultatif) Sélectionnez une interface sur laquelle aucun message PIM BSR ne sera envoyé ou reçu dans la section **Configure this ASA as a Border Bootstrap Router** (Configurer cet ASA en tant que routeur de démarrage frontalier).

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer une limite de multidiffusion

La portée des adresses définit des limites de domaine afin que les domaines dont les RP ont la même adresse IP n'empiètent pas l'un sur l'autre. La détermination de la portée est effectuée sur les limites du sous-réseau au sein des grands domaines et sur les limites entre le domaine et Internet.

Vous pouvez configurer une limite de portée administrative sur une interface pour les adresses de groupe de multidiffusion. L'IANA a désigné la plage d'adresses en multidiffusion de 239.0.0.0 à 239.255.255.255 comme adresses de portée administrative. Cette plage d'adresses peut être réutilisée dans des domaines administrés par différentes organisations. Les adresses seraient considérées comme locales et non uniques mondialement.

Une liste de contrôle d'accès standard définit la plage d'adresses concernées. Lorsqu'une limite est configurée, aucun paquet de données en multidiffusion ne peut traverser la limite dans aucune direction. La limite permet à la même adresse de groupe de multidiffusion d'être réutilisée dans différents domaines administratifs.

Vous pouvez configurer, examiner et filtrer les messages de découverte et d'annonce Auto-RP à la limite administrative. Toutes les annonces de plage de groupes Auto-RP des paquets Auto-RP qui sont refusées par l'ACL de frontière sont supprimées. Une annonce de plage de groupes Auto-RP est autorisée et transmise par la limite uniquement si toutes les adresses de la plage de groupes Auto-RP sont autorisées par la liste de contrôle d'accès (ACL) de limite. Si une adresse n'est pas autorisée, la plage complète de groupe est filtrée et supprimée du message Auto-RP avant que le message Auto-RP ne soit transféré.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **MBoundary (Limite de multidiffusion)**.

Le volet MBoundary (Limite de multidiffusion) vous permet de configurer une limite de multidiffusion pour les adresses de multidiffusion de portée administrative. Une limite de multidiffusion restreint les flux de paquets de données en multidiffusion et permet la réutilisation de la même adresse de groupe de multidiffusion dans différents domaines administratifs. Lorsqu'une limite de multidiffusion est définie sur une interface, seul le trafic en multidiffusion autorisé par la liste de contrôle d'accès du filtre passe par l'interface.

Étape 2 Cliquez sur **Edit**.

La boîte de dialogue Edit Boundary Filter (Modifier le filtre de limite) apparaît et affiche l'ACL du filtre de limite de multidiffusion. Vous pouvez ajouter et supprimer des entrées d'ACL de filtre de limite à l'aide de cette boîte de dialogue.

Lorsque la configuration du filtre de limite est appliquée à l'ASA, l'ACL apparaît dans la configuration d'exécution avec le nom *interface-name*_multicast, où *interface-name* est le nom de l'interface à laquelle le filtre de limite de multidiffusion est appliqué. Si une ACL porte déjà ce nom, un numéro est affecté au nom (par exemple, inside_multicast_1).

Étape 3 Dans la liste déroulante Interface, choisissez l'interface pour laquelle vous configurez l'ACL du filtre de limite de multidiffusion.

Étape 4 Cochez la case **Remove any Auto-RP group range** (Supprimer toute plage de groupes Auto-RP) pour filtrer les messages Auto-RP des sources refusées par l'ACL de la limite. Si la case **Remove any Auto-RP group range** (Supprimer toute plage de groupes Auto-RP) n'est pas cochée, tous les messages Auto-RP sont transmis.

Étape 5 Cliquez sur **OK**.

Supervision de PIM

Pour superviser ou désactiver diverses statistiques de routage PIM, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **BSR Router (Routeur BSR)**

Les renseignements relatifs à la configuration du routeur BSR s'affichent.

Étape 2 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **Multicast Routing Table (Table de routage de multidiffusion)**

Le contenu de la table de routage de multidiffusion s'affiche.

Étape 3 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **MFIB**

Les renseignements récapitulatifs sur le nombre d'entrées et d'interfaces de la base d'information de transfert multidiffusion PIM IPv4 s'affichent.

Étape 4 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **MFIB Active (MFIB active)**

Les renseignements récapitulatifs de la base d'information de transfert multidiffusion (MFIB) sur le débit auquel les sources de multidiffusion actives envoient des données aux groupes de multidiffusion s'affichent.

Étape 5 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **Group Map (Mappage de groupe)**

Les renseignements récapitulatifs de la base d'information de transfert multidiffusion (MFIB) sur le débit auquel les sources de multidiffusion actives envoient des données aux groupes de multidiffusion s'affichent.

a) Sélectionnez **RP Timers** (Minuteries RP) dans la liste déroulante **Select PIM Group** (Sélectionner un groupe PIM), pour afficher les renseignements sur la minuterie pour chaque mappage de groupe vers le mode PIM.

Étape 6 Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **PIM** > **Neighbors (Voisins)**

Les renseignements sur le voisin PIM (Protocole Independent Multicast) s'affichent.

Exemple de routage de multidiffusion

L'exemple suivant montre comment activer et configurer le routage de multidiffusion à l'aide de différents processus facultatifs :

1. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)**.

2. Dans le volet Multicast (Multidiffusion), cochez la case **Enable Multicast routing** (Activer le routage de multidiffusion), puis cliquez sur **Apply** (Appliquer).
3. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **MRoute**.
4. Cliquez sur **Add** ou **Edit** (Ajouter ou modifier) .

   La boîte de dialogue Add or Edit Multicast Route (Ajouter ou modifier une route de multidiffusion) s'affiche.

   Utilisez la boîte de dialogue Add Multicast Route (Ajouter une route de multidiffusion) pour ajouter une nouvelle route de multidiffusion statique à l'ASA. Utilisez la boîte de dialogue Edit Multicast Route (Modifier une route de multidiffusion) pour modifier une route de multidiffusion statique existante.
5. Dans le champ Source Address (Adresse source), saisissez l'adresse IP de la source de multidiffusion. Vous ne pouvez pas modifier cette valeur lors de la modification d'une route de multidiffusion statique existante.
6. Choisissez le masque réseau pour l'adresse IP de la source de multidiffusion dans la liste déroulante Source Mask (Masque source).
7. Dans la zone Incoming Interface (Interface entrante), cliquez sur le bouton radio **RPF Interface** (Interface RPF) pour choisir RPF pour transférer le routage ou sur le bouton radio **Interface Name** (Nom de l'interface), puis saisissez la commande suivante :
   - Dans le champ Source Interface (Interface source), choisissez l'interface entrante pour la route de multidiffusion dans la liste déroulante.
   - Dans le champ Destination Interface (Interface de destination), choisissez l'interface de destination à laquelle la route est transférée par l'intermédiaire de l'interface sélectionnée dans la liste déroulante.

Remarque Vous pouvez spécifier l'interface ou le voisin RPF, mais pas les deux en même temps.

8. Dans le champ Administrative Distance (Distance administrative), choisissez la distance administrative de la route de multidiffusion statique. Si la route de multidiffusion statique a la même distance administrative que la route de monodiffusion, la route de multidiffusion statique prévaut.
9. Cliquez sur **OK**.
10. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Multicast (Multidiffusion)** > **IGMP** > **Join Group (Groupe de jonction)**.

    Le volet Join Group (Groupe de jonction) apparaît.
11. Cliquez sur **Add** ou **Edit** (Ajouter ou modifier).

    La boîte de dialogue Add IGMP Join Group (Ajouter un groupe de jonction IGMP) vous permet de configurer une interface pour qu'elle soit membre d'un groupe de multidiffusion. La boîte de dialogue Edit IGMP Join Group (Modifier un groupe de jonction IGMP) vous permet de modifier les renseignements d'appartenance existants.

12. Dans le champ Interface Name (Nom de l'interface), choisissez le nom de l'interface dans la liste déroulante. Si vous modifiez une entrée existante, vous ne pouvez pas modifier cette valeur.
13. Dans le champ Multicast Group Address (Adresse de groupe de multidiffusion), saisissez l'adresse d'un groupe de multidiffusion auquel appartient l'interface. Les adresses de groupe valides sont comprises entre 224.0.0.0 et 239.255.255.255.
14. Cliquez sur **OK**.

Historique du routage de multidiffusion

Tableau 46 : Historique des fonctionnalités du routage de multidiffusion

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage de multidiffusion sur un tunnel de l'interface de tunnel virtuel statique	9.24(10)	Vous pouvez fournir en toute sécurité des applications de multidiffusion en temps réel, telles que la diffusion en flux continu de vidéos, les flux de données financières et la réplication de données sur votre infrastructure VPN en utilisant des tunnels IPsec configurés avec un VTI statique.
Prise en charge du routage de multidiffusion	7.0(1)	La prise en charge des données de routage de multidiffusion, de l'authentification, de la redistribution et de la surveillance des informations de routage à l'aide du protocole de routage de multidiffusion a été ajoutée. Nous avons introduit l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Multicast (Multidiffusion).
Prise en charge de la mise en grappe	9.0(1)	Une prise en charge a été ajoutée pour la mise en grappe.
Prise en charge du protocole PIM (Protocol Independent Multicast) en multidiffusion propre à la source (PIM-SSM)	9.5(1)	Une prise en charge a été ajoutée pour permettre aux paquets PIM-SSM de transiter lorsque le routage de multidiffusion est activé, sauf si l'ASA est le routeur de dernier saut. Cela permet une plus grande flexibilité dans le choix d'un groupe de multidiffusion tout en vous assurant une protection contre différentes attaques; les hôtes ne reçoivent que le trafic de sources explicitement demandées. Nous n'avons pas modifié d'écrans.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routeur de démarrage PIM (Protocol Independent Multicast)	9.5(2)	Une prise en charge a été ajoutée pour un nouveau modèle de sélection dynamique des points de rendez-vous (PRV) qui utilise des routeurs candidats pour la fonction Point de rendez-vous et pour le relais des informations Point de rendez-vous pour un groupe. Cette fonctionnalité fournit un moyen d'apprendre dynamiquement les points de rendez-vous (PRV), ce qui est tout à fait essentiel dans les grands réseaux complexes où un PRV peut périodiquement tomber en panne et se relancer. Nous avons introduit les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Multicast (Multidiffusion) > PIM > Bootstrap Router (Routeur de démarrage)
Limite igmp augmentée	9.15(1) *Également dans 9.12(4)*	La limite igmp a été augmentée de 500 à 5 000. Nous n'avons pas modifié d'écrans.



PARTIE VI

Serveurs AAA et base de données locale

- AAA et base de données locale, à la page 1065
- Serveurs RADIUS pour AAA, à la page 1079
- Serveurs TACACS+ pour AAA, à la page 1101
- Serveurs LDAP pour AAA, à la page 1109
- Serveurs Kerberos pour AAA, à la page 1121
- Configurer les serveurs RSA SecurID pour AAA, à la page 1127



CHAPITRE 38

AAA et base de données locale

Ce chapitre décrit l'authentification, l'autorisation et la traçabilité (AAA, prononcé « trois A »). Le protocole AAA regroupe un ensemble de services destinés à contrôler l'accès aux ressources informatiques, à appliquer des politiques, à évaluer l'utilisation et à fournir les renseignements nécessaires pour facturer les services. Ces processus sont considérés comme importants pour une gestion et une sécurité efficaces du réseau.

Ce chapitre décrit également comment configurer la base de données locale pour la fonctionnalité AAA. Pour les serveurs AAA externes, consultez le chapitre correspondant à votre type de serveur.

- À propos d'AAA et de la base de données locale, à la page 1065
- Lignes directrices relatives à la base de données locale, à la page 1070
- Ajouter un compte d'utilisateur à la base de données locale, à la page 1070
- Tester l'authentification et l'autorisation de la base de données locale, à la page 1072
- Supervision de la base de données locale, à la page 1073
- Historique de la base de données locale, à la page 1073

À propos d'AAA et de la base de données locale

Cette section décrit AAA et la base de données locale.

Authentification

L'authentification fournit un moyen d'identifier un utilisateur, généralement en demandant à l'utilisateur de saisir un nom d'utilisateur et un mot de passe valides avant que l'accès ne soit accordé. Le serveur AAA compare les renseignements d'authentification d'un utilisateur à ceux d'autres utilisateurs stockés dans une base de données. Si les renseignements d'authentification correspondent, l'utilisateur est autorisé à accéder au réseau. Dans le cas contraire, l'authentification échoue et l'accès au réseau est refusé.

Vous pouvez configurer l'ASA pour authentifier les éléments suivants :

- Toutes les connexions administratives à l'ASA, y compris les sessions suivantes :
  - Telnet
  - SSH
  - Console de série
  - ASDM à l'aide de HTTPS

- Accès à la gestion du VPN

- La commande **enable**
- Accès au réseau
- Accès VPN

Autorisation

L'autorisation est le processus d'application des politiques : qui détermine les types d'activités, de ressources ou de services auxquels un utilisateur est autorisé à accéder. Une fois qu'un utilisateur est authentifié, cet utilisateur peut être autorisé pour différents types d'accès ou d'activités.

Vous pouvez configurer l'ASA pour autoriser les éléments suivants :

- Commandes de gestion
- Accès au réseau
- Accès VPN

Comptabilité

La comptabilité mesure les ressources qu'un utilisateur consomme lors de l'accès, qui peuvent inclure la durée du système ou la quantité de données qu'un utilisateur a envoyées ou reçues au cours d'une session. La comptabilisation est effectuée au moyen de la journalisation des statistiques de session et des renseignements d'utilisation, qui sont utilisés pour les activités de contrôle des autorisations, de facturation, d'analyse des tendances, d'utilisation des ressources et de planification de la capacité.

Interaction entre authentification, autorisation et traçabilité

Vous pouvez utiliser l'authentification seule ou avec l'autorisation et la comptabilité. L'autorisation nécessite toujours qu'un utilisateur soit d'abord authentifié. Vous pouvez utiliser la comptabilité seule ou avec l'authentification et l'autorisation.

Serveurs et groupes de serveurs AAA

Le serveur AAA est un serveur de réseau utilisé pour le contrôle d'accès. L'authentification identifie l'utilisateur. L'autorisation met en œuvre des politiques qui déterminent les ressources et les services auxquels un utilisateur authentifié peut accéder. La comptabilité fait le suivi des ressources de temps et de données utilisées pour la facturation et l'analyse.

Si vous souhaitez utiliser un serveur AAA externe, vous devez d'abord créer un groupe de serveurs AAA pour le protocole utilisé par le serveur externe et ajouter le serveur au groupe. Vous pouvez créer plusieurs groupes par protocole et des groupes distincts pour tous les protocoles que vous souhaitez utiliser. Chaque groupe de serveurs est propre à un type de serveur ou de service.

Consultez les rubriques suivantes pour en savoir plus sur la création des groupes :

- Configurer les groupes de serveurs RADIUS, à la page 1092

- Configurer les groupes de serveurs TACACS+, à la page 1103
- Configurer les groupes de serveurs LDAP, à la page 1115
- Configurer les groupes de serveurs AAA Kerberos, à la page 1121
- Configurer les groupes de serveurs RSA SecurID pour AAA, à la page 1128

Consultez le guide de configuration de VPN pour en savoir plus sur l'utilisation de la délégation sous contraintes de Kerberos et du formulaire HTTP.

Le tableau suivant résume les types de serveurs pris en charge et leurs utilisations, y compris la base de données locale.

Tableau 47 : Services pris en charge pour les serveurs AAA

Type de serveur et service	Authentification	Autorisation	Gestion de comptes
Base de données locale			
Administrateurs	Oui	Oui	Non
Utilisateurs VPN	Oui	Non	Non
Sessions de pare-feu (règles AAA)	Oui	Oui	Non
RADIUS			
Administrateurs	Oui	Oui	Oui
Utilisateurs VPN	Oui	Oui	Oui
Sessions de pare-feu (règles AAA)	Oui	Oui	Oui
TACACS+			
Administrateurs	Oui	Oui	Oui
Utilisateurs VPN	Oui	Non	Oui
Sessions de pare-feu (règles AAA)	Oui	Oui	Oui
LDAP			
Administrateurs	Oui	Non	Non
Utilisateurs VPN	Oui	Oui	Non
Sessions de pare-feu (règles AAA)	Oui	Non	Non
Kerberos			
Administrateurs	Oui	Non	Non

Type de serveur et service	Authentification	Autorisation	Gestion de comptes
Utilisateurs VPN	Oui	Non	Non
Sessions de pare-feu (règles AAA)	Oui	Non	Non
SDI (RSA SecurID)			
Administrateurs	Oui	Non	Non
Utilisateurs VPN	Oui	Non	Non
Sessions de pare-feu (règles AAA)	Oui	Non	Non
Formulaire HTTP			
Administrateurs	Non	Non	Non
Utilisateurs VPN	Oui	Non	Non
Sessions de pare-feu (règles AAA)	Non	Non	Non

Notes

- RADIUS : la comptabilisation des administrateurs n'inclut pas la comptabilisation des commandes.
- RADIUS : l'autorisation des sessions de pare-feu est prise en charge uniquement avec les listes d'accès spécifiques à l'utilisateur, qui sont reçues ou spécifiées dans une réponse à la demande d'authentification RADIUS.
- TACACS+ : la comptabilisation des administrateurs comprend la comptabilisation des commandes.
- Formulaire HTTP : opérations d'authentification et SSO pour les sessions utilisateur du SSL VPN sans client uniquement.

À propos de la base de données locale

L'ASA gère une base de données locale que vous pouvez remplir avec les profils d'utilisateurs. Vous pouvez utiliser une base de données locale au lieu de serveurs AAA pour assurer l'authentification, l'autorisation et la traçabilité des utilisateurs.

Vous pouvez utiliser la base de données locale pour les fonctions suivantes :

- Accès à ASDM par utilisateur
- Authentification de la console
- Authentification Telnet et SSH
- Authentification de la commande **enable**

  Ce paramètre est réservé à l'accès à l'interface de ligne de commande et n'influe pas sur la connexion à Cisco ASDM.

- Autorisation de commande

  Si vous activez l'autorisation de commande à l'aide de la base de données locale, l'ASA fait référence au niveau de privilège de l'utilisateur pour déterminer quelles commandes sont disponibles. Sinon, le niveau de privilège n'est généralement pas utilisé. Par défaut, toutes les commandes sont de niveau de privilège 0 ou de niveau 15. ASDM vous permet d'activer trois niveaux de privilèges prédéfinis, avec des commandes attribuées au niveau 15 (Admin), au niveau 5 (Lecture seule) et au niveau 3 (Superviser uniquement). Si vous utilisez les niveaux prédéfinis, affectez des utilisateurs à l'un de ces trois niveaux de privilège.

- Authentification d'accès au réseau
- Authentification du client VPN

Pour le mode de contexte multiple, vous pouvez configurer les noms d'utilisateur dans l'espace d'exécution du système pour fournir des connexions individuelles au niveau de l'interface de ligne de commande à l'aide de la commande **login**; cependant, vous ne pouvez pas configurer de règles AAA qui utilisent la base de données locale dans l'espace d'exécution du système.

Remarque Vous ne pouvez pas utiliser la base de données locale pour l'autorisation d'accès au réseau.

Prise en charge du basculement

La base de données locale peut servir de méthode de secours pour plusieurs fonctions. Ce comportement est conçu pour vous aider à éviter le verrouillage accidentel de l'ASA.

Lorsqu'un utilisateur se connecte, les serveurs du groupe sont accessibles un par un en commençant par le premier serveur que vous spécifiez dans la configuration, jusqu'à ce qu'un serveur réponde. Si tous les serveurs du groupe sont indisponibles, l'ASA essaie la base de données locale si vous l'avez configurée comme méthode de secours (pour l'authentification et l'autorisation de gestion uniquement). Si vous n'avez pas de méthode de secours, l'ASA continue d'essayer les serveurs AAA.

Pour les utilisateurs qui ont besoin d'une prise en charge de secours, nous recommandons que leurs noms d'utilisateur et mots de passe dans la base de données locale correspondent à leurs noms d'utilisateur et mots de passe sur les serveurs AAA. Cette pratique offre une prise en charge de secours transparente. Étant donné que l'utilisateur ne peut pas déterminer si un serveur AAA ou la base de données locale fournit le service, l'utilisation de noms d'utilisateur et de mots de passe sur des serveurs AAA qui sont différents de ceux de la base de données locale signifie que l'utilisateur ne peut pas être certain du nom d'utilisateur et du mot de passe à fournir.

La base de données locale prend en charge les fonctions de secours suivantes :

- Console et activation de l'authentification par mot de passe : si les serveurs du groupe sont tous indisponibles, l'ASA utilise la base de données locale pour authentifier l'accès administratif, qui peut également inclure l'activation de l'authentification par mot de passe.
- Autorisation de commande : si les serveurs TACACS+ du groupe sont tous indisponibles, la base de données locale est utilisée pour autoriser les commandes en fonction des niveaux de privilège.
- Authentification et autorisation VPN : l'authentification et l'autorisation VPN sont prises en charge pour permettre l'accès à distance à l'ASA si les serveurs AAA qui prennent normalement en charge ces services VPN ne sont pas disponibles. Lorsqu'un client VPN d'un administrateur spécifie un groupe de tunnels

configuré pour un basculement vers la base de données locale, le tunnel VPN peut être établi même si le groupe de serveurs AAA n'est pas disponible, à condition que la base de données locale soit configurée avec les attributs nécessaires.

Fonctionnement du basculement avec plusieurs serveurs dans un groupe

Si vous configurez plusieurs serveurs dans un groupe de serveurs et que vous activez le basculement vers la base de données locale pour le groupe de serveurs, le basculement se produit lorsqu'aucun serveur du groupe ne répond à la demande d'authentification de l'ASA. Par exemple, envisagez le scénario suivant :

Vous configurez un groupe de serveurs LDAP avec deux serveurs Active Directory, le serveur 1 et le serveur 2, dans cet ordre. Lorsque l'utilisateur distant se connecte, l'ASA tente de s'authentifier auprès du serveur 1.

Si le serveur 1 répond par un échec d'authentification (par exemple, un utilisateur introuvable), l'ASA ne tente pas de s'authentifier auprès du serveur 2.

Si le serveur 1 ne répond pas dans le délai d'expiration (ou si le nombre de tentatives d'authentification dépasse le maximum configuré), l'ASA essaie le serveur 2.

Si les deux serveurs du groupe ne répondent pas et que l'ASA est configuré pour revenir à la base de données locale, l'ASA tente de s'authentifier auprès de la base de données locale.

Remarque Par défaut, un client RADIUS envoie trois demandes avant d'expirer. Lorsque le client tente d'établir une connexion SSH, la demande est envoyée à un serveur à la fois. À l'expiration des demandes, le serveur est marqué comme ayant ÉCHOUÉ. La prochaine demande RADIUS est envoyée au serveur ACTIF suivant, marquant par la suite tous les serveurs comme ayant ÉCHOUÉ et revenant finalement à l'authentification LOCALE (si elle est configurée). Les serveurs marqués comme ayant ÉCHOUÉ finissent par se rétablir et sont rendus ACTIFS. Dans ce cas, si vous avez 3 ou 4 serveurs dans le groupe, vous pourriez observer des problèmes de connexion intermittents.

Lignes directrices relatives à la base de données locale

Assurez-vous d'empêcher un verrouillage de l'ASA lorsque vous utilisez la base de données locale pour l'authentification ou l'autorisation.

Ajouter un compte d'utilisateur à la base de données locale

Pour ajouter un utilisateur à la base de données locale, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add User Account-Identity** (Ajouter une identité de compte d'utilisateur) apparaît.

Étape 2 Saisissez un nom d'utilisateur de 4 à 64 caractères.

Étape 3 (Facultatif) Saisissez un mot de passe compris entre 8 et 127 caractères.

Les valeurs des mots de passe respectent la casse. Il peut s'agir de n'importe quelle combinaison de caractères imprimables ASCII (codes 32 à 126), avec les exceptions suivantes :

- Aucun espace
- Aucun point d'interrogation
- Il est interdit d'utiliser trois caractères ASCII (ou plus) qui se suivent ou qui se répètent. Par exemple, les mots de passe suivants seront refusés :
  - **abc**utilisateur1
  - utilisateur**543**
  - utilisateur**aaaa**
  - utilisateur2**666**

Le champ affiche uniquement des astérisques. Par exemple, vous souhaiterez peut-être créer un nom d'utilisateur sans mot de passe si vous utilisez l'authentification par clé publique SSH.

Remarque Pour configurer le mot de passe d'activation à partir du volet **User Accounts** (Comptes d'utilisateurs), modifiez le mot de passe de l'utilisateur enable_15. L'utilisateur enable_15 est toujours présent dans le volet **User Accounts** (Comptes d'utilisateurs) et représente le nom d'utilisateur par défaut. Cette méthode de configuration du mot de passe d'activation est la seule méthode disponible dans ASDM pour la configuration système. Si vous avez configuré d'autres mots de passe de niveau d'activation au niveau de l'interface de ligne de commande (par exemple, le mot de passe enable 10), ces utilisateurs sont répertoriés comme enable_10, et ainsi de suite.

Étape 4 Entrez le mot de passe de nouveau.

Pour des raisons de sécurité, seuls les astérisques apparaissent dans les champs du mot de passe.

Étape 5 Cochez la case **User authenticated using MSCHAP** (Utilisateur authentifié à l'aide de MSCHAP) si vous utilisez MSCHAP pour l'authentification.

Étape 6 Définissez le niveau d'accès de gestion d'un utilisateur dans la zone **Access Restriction** (Restriction d'accès). Vous devez d'abord activer l'autorisation de gestion en cliquant sur l'option **Perform authorization for exec shell access** (Effectuer l'autorisation pour l'accès au shell d'exécution) sous l'onglet **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Authorisation)**.

Choisissez une des options suivantes :

- **Full Access (ASDM, Telnet, SSH and console)** (Accès complet (ASDM, Telnet, SSH et console)) : si vous configurez l'authentification pour l'accès de gestion à l'aide de la base de données locale, cette option permet à l'utilisateur d'utiliser ASDM, SSH, Telnet et le port de console. Si vous activez également l'authentification, l'utilisateur peut accéder au mode de configuration globale.
  - **Privilege Level** (Niveau de privilège) : définit le niveau de privilège pour ASDM et l'autorisation de commande locale. La plage va de 0 (le plus bas) à 15 (le plus élevé). Spécifiez 15 pour accorder un accès administrateur sans restriction. Les rôles ASDM prédéfinis utilisent 15 pour l'administration,

5 pour la lecture seule et 3 pour la surveillance uniquement (ce qui limite l'utilisateur aux volets Home (Accueil) et Monitoring (Supervision)).

- **CLI login prompt for SSH, Telnet and console (no ASDM access)** (Invite de connexion à l'interface de ligne de commande pour SSH, Telnet et la console (sans accès ASDM)) : si vous configurez l'authentification pour l'accès de gestion à l'aide de la base de données locale, cette option permet à l'utilisateur d'utiliser SSH, Telnet et le port de console. L'utilisateur ne peut pas utiliser ASDM pour la configuration (si vous configurez l'authentification HTTP). La surveillance ASDM est autorisée. Si vous configurez également l'authentification de l'activation, l'utilisateur ne peut pas accéder au mode de configuration globale.
- **No ASDM, SSH, Telnet, or console access** (Aucun accès ASDM, SSH, Telnet ou à la console) : si vous configurez l'authentification pour l'accès de gestion à l'aide de la base de données locale, cette option empêche l'utilisateur d'accéder à toute méthode d'accès de gestion pour laquelle vous avez configuré l'authentification (à l'exception de l'option de série; l'accès en série est autorisé).

Étape 7 (Facultatif) Pour activer l'authentification par clé publique pour les connexions SSH à l'ASA par utilisateur, consultez Configurer l'accès HTTPS pour ASDM, autres clients, à la page 1136.

Étape 8 Cliquez sur **VPN Policy** (Politique VPN) pour configurer les attributs de la politique VPN pour cet utilisateur. Consultez le guide de configuration du VPN.

Étape 9 Cliquez sur **Apply** (Appliquer).

L'utilisateur est ajouté à la base de données locale et les modifications sont enregistrées dans la configuration en cours d'exécution.

Astuces Vous pouvez rechercher du texte spécifique dans chaque colonne du volet **Configuration** > **Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs)**. Saisissez le texte que vous souhaitez localiser dans la zone **Find** (Rechercher), puis cliquez sur la flèche **vers le haut** ou **vers le bas**. Vous pouvez également utiliser l'astérisque (« * ») et le point d'interrogation (« ? ») comme caractères génériques dans la recherche de texte.

Tester l'authentification et l'autorisation de la base de données locale

Pour déterminer si l'ASA peut communiquer avec une base de données locale et authentifier ou autoriser un utilisateur, procédez comme suit :

Procédure

Étape 1 Dans le tableau **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs AAA)** > **AAA Server Groups (Groupes de serveurs AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**, cliquez sur le groupe de serveurs dans lequel se trouve le serveur.

Étape 2 Cliquez sur le serveur que vous souhaitez tester dans le tableau **Servers in the Selected Group** (Serveurs du groupe sélectionné).

Étape 3 Cliquez sur **Test**.

La boîte de dialogue **Test AAA Server** (Tester un serveur AAA) s'affiche pour le groupe de serveurs sélectionné.

Étape 4 Cliquez sur le type de test que vous souhaitez effectuer : **Authentication** (Authentification) ou **Authorization** (Autorisation).

Étape 5 Saisissez un nom d'utilisateur.

Étape 6 Si vous testez l'authentification, saisissez le mot de passe correspondant au nom d'utilisateur.

Étape 7 Cliquez sur **OK**.

L'ASA envoie un message de test d'authentification ou d'autorisation au serveur. Si le test échoue, ASDM affiche un message d'erreur.

Supervision de la base de données locale

Consultez les commandes suivantes pour superviser la base de données locale :

- **Monitoring (Supervision) > Properties (Propriétés) > AAA Servers (Serveurs AAA)**

  Ce volet affiche les statistiques du serveur AAA.

- **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

Historique de la base de données locale

Tableau 48 : Historique de la base de données locale

Nom de la caractéristique	Versions de plateforme	Description
Configuration de la base de données locale pour AAA	7.0(1)	Décrit comment configurer la base de données locale pour une utilisation AAA. Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Server Groups Configuration (Configuration des groupes de serveurs AAA) > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs).

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de l'authentification par clé publique SSH	9.1(2)	Vous pouvez désormais activer l'authentification par clé publique pour les connexions SSH à l'ASA par utilisateur. Vous pouvez spécifier une clé formatée de fichier de clé publique (PKF) ou une clé Base64. La clé PKF peut comporter jusqu'à 4 096 bits. Utilisez le format PKF pour les clés qui sont trop grandes pour la prise en charge ASA du format Base64 (jusqu'à 2 048 bits). Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs) > Edit User Account (Modifier le compte d'utilisateur) > Public Key Authentication (Authentification par clé publique) Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs) > Edit User Account (Modifier le compte d'utilisateur) > Public Key Using PKF (Clé publique utilisant PKF) *Également disponible dans 8.4(4.1); la prise en charge du format de clé PKF uniquement dans 9.1(2).*
Prise en charge de mots de passe plus longs pour les mots de passe locaux **username** et **enable** (jusqu'à 127 caractères)	9.6(1)	Vous pouvez désormais créer des mots de passe **username** et **enable** locaux jusqu'à 127 caractères (l'ancienne limite était de 32). Lorsque vous créez un mot de passe de plus de 32 caractères, il est stocké dans la configuration à l'aide d'un hachage PBCDF2 (Password-Based Key Derivation Function 2). Les mots de passe plus courts continuent d'utiliser la méthode de hachage basée sur MD5. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)** > **Enable Password (Mot de passe d'activation)** **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)** > **Identity (Identité)**

Nom de la caractéristique	Versions de plateforme	Description
Améliorations de l'authentification par clé publique SSH	9.6(2)	Dans les versions antérieures, vous pouviez activer l'authentification par clé publique SSH sans activer également l'authentification SSH AAA avec la base de données d'utilisateurs locale . La configuration est désormais modifiée de manière à ce que vous deviez explicitement activer l'authentification SSH AAA. Pour empêcher les utilisateurs d'utiliser un mot de passe au lieu de la clé privée, vous pouvez désormais créer un nom d'utilisateur sans mot de passe défini. Nous avons modifié les écrans suivants : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)**
Hachage PBKDF2 pour tous les mots de passe locaux **username** et **enable**	9.7(1)	Les mots de passe locaux **username** et **enable** de toutes les longueurs sont stockés dans la configuration à l'aide du hachage PBKDF2 (Password-Based Key Derivation Function 2). Auparavant, les mots de passe de 32 caractères et moins utilisaient la méthode de hachage basée sur MD5. Les mots de passe existants continuent d'utiliser le hachage basé sur MD5, sauf si vous entrez un nouveau mot de passe. Consultez le chapitre « Logiciels et configurations » du Guide de configuration des opérations générales pour connaître les lignes directrices relatives à la rétrogradation. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)** > **Enable Password (Mot de passe d'activation)** **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)** > **Identity (Identité)**

Nom de la caractéristique	Versions de plateforme	Description
Authentification distincte pour les utilisateurs disposant d'une authentification par clé publique SSH et les utilisateurs disposant de mots de passe	9.6(3)/9.8(1)	Dans les versions antérieures à 9.6(2), vous pouviez activer l'authentification par clé publique SSH (**ssh authentication**) sans activer explicitement l'authentification SSH AAA avec la base de données des utilisateurs locale (**aaa authentication ssh console LOCAL**). Dans 9.6(2), l'ASA vous a demandé d'activer explicitement l'authentification SSH AAA. Dans cette version, vous n'avez plus à activer explicitement l'authentification SSH AAA; lorsque vous configurez la commande **ssh authentication** pour un utilisateur, l'authentification locale est activée par défaut pour les utilisateurs avec ce type d'authentification. De plus, lorsque vous configurez explicitement l'authentification SSH AAA, cette configuration s'applique uniquement aux noms d'utilisateur avec *mots de passe*, et vous pouvez utiliser n'importe quel type de serveur AAA (**aaa authentication ssh console radius_1**, par exemple). Par exemple, certains utilisateurs peuvent utiliser l'authentification par clé publique à l'aide de la base de données locale et d'autres utilisateurs peuvent utiliser des mots de passe avec RADIUS. Nous n'avons pas modifié d'écrans.
Exigences relatives à l'utilisateur local et au mot de passe d'activation	9.17(1)	Pour les utilisateurs locaux et le mot de passe d'activation, les exigences de mot de passe suivantes ont été ajoutées : • Longueur du mot de passe : au moins 8 caractères. Auparavant, le minimum était de 3 caractères. • Caractères répétitifs et séquentiels : trois caractères ASCII ou plus consécutifs ne sont pas autorisés. Par exemple, les mots de passe suivants seront refusés : • **abc**utilisateur1 • utilisateur**543** • utilisateur**aaaa** • utilisateur2**666** Écrans Nouveaux ou modifiés : • **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)**

Nom de la caractéristique	Versions de plateforme	Description
Modifications du verrouillage de l'utilisateur local	9.17(1)	L'ASA peut verrouiller les utilisateurs locaux après un nombre configurable de tentatives de connexion échouées. Cette fonctionnalité ne s'applique pas aux utilisateurs ayant le niveau de privilège 15. De plus, un utilisateur serait verrouillé indéfiniment jusqu'à ce qu'un administrateur déverrouille son compte. Désormais, les utilisateurs seront déverrouillés après 10 minutes, à moins qu'un administrateur n'utilise la commande **clear aaa local user lockout** avant. Les utilisateurs ayant le niveau de privilège 15 sont également concernés par le paramètre de verrouillage. Commandes nouvelles ou modifiées : **aaa local authentication attempts max-fail** , **show aaa local user**
Invite de modification du mot de passe SSH et Telnet	9.17(1)	La première fois qu'un utilisateur local se connecte à l'ASA à l'aide de SSH ou de Telnet, il est invité à changer de mot de passe. Il sera également invité à se connecter pour la première fois après qu'un administrateur aura modifié son mot de passe. Si l'ASA se recharge, les utilisateurs ne seront pas invités, même s'il s'agit de leur première connexion. Commandes nouvelles ou modifiées : **show aaa local user**



CHAPITRE 39

Serveurs RADIUS pour AAA

Ce chapitre décrit comment configurer les serveurs RADIUS pour AAA.

- À propos des serveurs RADIUS pour AAA, à la page 1079
- Lignes directrices relatives aux serveurs RADIUS pour AAA, à la page 1091
- Configurer les serveurs RADIUS pour AAA, à la page 1092
- Tester l'authentification et l'autorisation du serveur RADIUS, à la page 1098
- Supervision des serveurs RADIUS pour AAA, à la page 1099
- Historique des serveurs RADIUS pour AAA, à la page 1099

À propos des serveurs RADIUS pour AAA

L'ASA prend en charge les serveurs RADIUS conformes à la norme RFC suivants pour AAA :

- Cisco Secure ACS 3.2, 4.0, 4.1, 4.2 et 5.x
- Cisco Identity Services Engine (ISE)
- RSA RADIUS dans RSA Authentication Manager 5.2, 6.1, 7.x, 8.x
- Microsoft

Méthodes d'authentification prises en charge

L'ASA prend en charge les méthodes d'authentification suivantes avec les serveurs RADIUS :

- PAP : pour tous les types de connexion.
- CHAP et MS-CHAPv1 : pour les connexions L2TP-over-IPsec.
- MS-CHAPv2 : pour les connexions L2TP sur IPsec et pour les connexions d'accès à distance IPsec normales lorsque la fonctionnalité de gestion des mots de passe est activée. Vous pouvez également utiliser MS-CHAPv2 avec des connexions sans client.
- Modes de mandataire pour l'authentification : pour les connexions RADIUS à Active-Directory, RADIUS à RSA/SDI, RADIUS à serveur de jeton et RSA/SDI à RADIUS.

Remarque Pour activer MS-CHAPv2 comme protocole utilisé entre l'ASA et le serveur RADIUS pour une connexion VPN, la gestion des mots de passe doit être activée dans les attributs généraux du groupe de tunnels. L'activation de la gestion des mots de passe génère une demande d'authentification MS-CHAPv2 de l'ASA au serveur RADIUS. Consultez la description de la commande **password-management** pour en savoir plus.

Si vous utilisez la double authentification et activez la gestion des mots de passe dans le groupe de tunnels, les demandes d'authentification principale et secondaire incluent les attributs de demande MS-CHAPv2. Si un serveur RADIUS ne prend pas en charge MS-CHAPv2, vous pouvez configurer ce serveur pour envoyer une demande d'authentification non MS-CHAPv2 à l'aide de la commande **no mschapv2-capable**.

Autorisation des utilisateurs pour les connexions VPN

L'ASA peut utiliser des serveurs RADIUS pour l'autorisation des utilisateurs d'accès à distance VPN et des sessions de mandataire direct de pare-feu à l'aide d'ACL dynamiques ou de noms d'ACL par utilisateur. Pour mettre en œuvre des ACL dynamiques, vous devez configurer le serveur RADIUS pour les prendre en charge. Lorsque l'utilisateur s'authentifie, le serveur RADIUS envoie une ACL téléchargeable ou un nom d'ACL à l'ASA. L'accès à un service donné est autorisé ou refusé par l'ACL. L'ASA supprime l'ACL lorsque la session d'authentification expire.

En plus des ACL, l'ASA prend en charge de nombreux autres attributs pour l'autorisation et la définition des autorisations pour l'accès à distance au VPN et les sessions de mandataire direct par le pare-feu.

Ensembles d'attributs RADIUS pris en charge

L'ASA prend en charge les ensembles d'attributs RADIUS suivants :

- Attributs d'authentification définis dans les RFC 2138 et 2865.
- Attributs de traçabilité définis dans les RFC 2139 et 2866.
- Attributs RADIUS pour la prise en charge du protocole tunnelé, définis dans les RFC 2868 et 6929.
- Attributs spécifiques au fournisseur (VSA) Cisco IOS, identifiés par l'ID de fournisseur RADIUS 9.
- VSA liés au VPN Cisco, identifiés par l'ID de fournisseur RADIUS 3076.
- VSA Microsoft, définis dans la RFC 2548.

Attributs d'autorisation RADIUS pris en charge

L'autorisation désigne le processus d'application d'autorisations ou d'attributs. Un serveur RADIUS défini comme serveur d'authentification applique des autorisations ou des attributs s'ils sont configurés. Ces attributs ont l'ID de prestataire 3076.

Le tableau suivant répertorie les attributs RADIUS pris en charge qui peuvent être utilisés pour l'autorisation de l'utilisateur.



Remarque Les noms d'attributs RADIUS ne contiennent pas le préfixe cVPN3000. Cisco Secure ACS 4.x prend en charge cette nouvelle nomenclature, mais les noms d'attributs dans les versions ACS antérieures à la version 4.0 incluent toujours le préfixe cVPN3000. Les ASA appliquent les attributs RADIUS en fonction de l'ID numérique de l'attribut, et non du nom de l'attribut.

Tous les attributs répertoriés dans le tableau suivant sont des attributs en aval envoyés du serveur RADIUS à l'ASA, à l'exception des numéros d'attribut suivants : 146, 150, 151 et 152. Ces numéros d'attribut sont des attributs en amont qui sont envoyés de l'ASA au serveur RADIUS. Les attributs RADIUS 146 et 150 sont envoyés de l'ASA au serveur RADIUS pour les demandes d'authentification et d'autorisation. Les quatre attributs précédemment répertoriés sont envoyés de l'ASA au serveur RADIUS pour les demandes de démarrage, de mise à jour provisoire et d'arrêt de gestion. Les attributs RADIUS en amont 146, 150, 151 et 152 ont été introduits dans la version 8.4(3).

Tableau 49 : Attributs d'autorisation RADIUS pris en charge

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Heures d'accès	O	1	Chaîne	Unique	Nom de la plage temporelle, par exemple, Heures ouvrables
Liste d'accès entrant	O	86	Chaîne	Unique	ID d'ACL
Liste d'accès sortante	O	87	Chaîne	Unique	ID d'ACL
Ensembles des adresses	O	217	Chaîne	Unique	Nom de l'ensemble d'adresses IP locales
Allow-Network-Extension-Mode	O	64	Booléen	Unique	0 = Désactivé 1 = Activé
Authenticated-User-Idle-Timeout	O	50	nombre entier	Unique	1 à 35791394 minutes
Authorization-DN-Field	O	67	Chaîne	Unique	Valeurs possibles : UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER, use-entire-name
Authorization-Required		66	nombre entier	Unique	0 = non 1 = oui
Authorization-Type	O	65	nombre entier	Unique	0 = Aucun 1 = RADIUS 2 = LDAP
Banner1	O	15	Chaîne	Unique	Chaîne de caractères de bannière à afficher pour les sessions d'accès à distance VPN Cisco : IPsec IKEv1, Secure Client (services client sécurisés) SSL-TLS/DTLS/IKEv2 et Clientless SSL

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Banner2	O	36	Chaîne	Unique	Chaîne de caractères de bannière à afficher pour les sessions d'accès à distance VPN Cisco : IPsec IKEv1, Secure Client (services client sécurisés) SSL-TLS/DTLS/IKEv2 et Clientless SSL La chaîne Bannière2 est concaténée à la chaîne Bannière1, si elle est configurée.
Cisco-IP-Phone-Bypass	O	51	nombre entier	Unique	0 = Désactivé 1 = Activé
Cisco-LEAP-Bypass	O	75	nombre entier	Unique	0 = Désactivé 1 = Activé
Type de client	O	150	nombre entier	Unique	1 = Cisco VPN Client (IKEv1) 2 = Secure Client (services client sécurisés) SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 = Secure Client (services client sécurisés) IPsec VPN (IKEv2)
Client-Type-Version-Limiting	O	77	Chaîne	Unique	Chaîne du numéro de version de VPN IPSec
DHCP-Network-Scope	O	61	Chaîne	Unique	Adresse IP
Extended-Authentication-On-Rekey	O	122	nombre entier	Unique	0 = Désactivé 1 = Activé
Framed-Interface-Id	O	96	Chaîne	Unique	ID de l'interface IPv6 affectée. Se combine avec Framed-IPv6-Prefix pour créer une adresse IPv6 complète. Par exemple : Framed-Interface-ID=1:1:1:1 combiné avec Framed-IPv6-Prefix= 2001:0db8::/64 donne l'adresse IP attribuée 2001:0db8::1:1:1:1.
Framed-IPv6-Prefix	O	97	Chaîne	Unique	Préfixe et longueur IPv6 affectées. À combiner avec Framed-Interface-Id pour créer une adresse IPv6 complète. Par exemple : prefix 2001:0db8::/64 combiné avec Framed-Interface-Id=1:1:1:1:1 donne l'adresse IP 2001:0db8::1:1:1:1. Vous pouvez utiliser cet attribut pour attribuer une adresse IP sans utiliser Framed-Interface-Id, en attribuant l'adresse IPv6 complète avec la longueur de préfixe /128, par exemple, Framed-IPv6-Prefix=2001:0db8::1/128.

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Politique de groupe	O	25	Chaîne	Unique	Définit la politique de groupe pour la session VPN d'accès à distance. Pour les versions 8.2.x et ultérieures, utilisez cet attribut au lieu de IETF-Radius-Class. Vous pouvez utiliser l'un des formats suivants : • *nom de la politique de groupe* • OU=*nom de la politique de groupe* • OU=*nom de la politique de groupe*;
IE-Proxy-Bypass-Local		83	nombre entier	Unique	0 = aucun 1 = local
IE-Proxy-Exception-List		82	Chaîne	Unique	Nouvelle liste de domaines DNS séparés par des lignes (\n)
URL-PAC-IE-Proxy	O	133	Chaîne	Unique	Chaîne d'adresse PAC
IE-Proxy-Server		80	Chaîne	Unique	Adresse IP
IE-Proxy-Server-Policy		81	nombre entier	Unique	1 = Aucune modification 2 = Aucun mandataire 3 = Détection automatique 4 = Utiliser le paramètre du concentrateur
IKE-KeepAlive-Confidence-Interval	O	68	nombre entier	Unique	10 à 300 secondes
IKE-Keepalive-Retry-Interval	O	84	nombre entier	Unique	2 à 10 secondes
IKE-Keep-Alives	O	41	Booléen	Unique	0 = Désactivé 1 = Activé
Intercept-DHCP-Configure-Msg	O	62	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Allow-Passwd-Store	O	16	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Authentication		13	nombre entier	Unique	0 = Aucun 1 = RADIUS 2 = LDAP (autorisation seulement) 3 = Domaine NT 4 = SDI 5 = Interne 6 = RADIUS avec expiration 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	O	42	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Backup-Server-List	O	60	Chaîne	Unique	Adresses du serveur (délimitées par un espace)
IPsec-Backup-Servers	O	59	Chaîne	Unique	1 = Utiliser la liste configurée par le client 2 = Désactiver et effacer la liste du client 3 = Utiliser la liste du serveur de sauvegarde
IPsec-Client-Firewall-Filter-Name		57	Chaîne	Unique	Spécifie le nom du filtre à envoyer au client en tant que politique de pare-feu

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IPsec-Client-Firewall-Filter-Optional	O	58	nombre entier	Unique	0 = obligatoire 1 = facultatif
IPsec-Default-Domain	O	28	Chaîne	Unique	Spécifie le nom de domaine par défaut à envoyer au client (1 à 255 caractères).
IPsec-IKE-Peer-ID-Check	O	40	nombre entier	Unique	1 = Obligatoire 2 = Si pris en charge par le certificat homologue 3 = Ne pas vérifier
IPsec-IP-Compression	O	39	nombre entier	Unique	0 = Désactivé 1 = Activé
IPsec-Mode-Config	O	31	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Over-UDP	O	34	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Over-UDP-Port	O	35	nombre entier	Unique	4001à 49151. La valeur par défaut est 10 000.
IPsec-Required-Client-Firewall-Capability	O	56	nombre entier	Unique	0 = Aucune 1 = Politique définie par le micro-logiciel Are You There (Ayt) distant 2 = Politique transmise au CPP 4 = Politique du serveur
IPsec-Sec-association		12	Chaîne	Unique	Nom de l'association de sécurité
IPsec-Split-DNS-Names	O	29	Chaîne	Unique	Spécifie la liste des noms de domaines secondaires à envoyer au client (1 à 255 caractères).
IPsec-Split-Tunneling-Policy	O	55	nombre entier	Unique	0 = Aucun tunnellisation fractionnée 1 = Tunnellisation fractionnée 2 = LAN local autorisé
IPsec-Split-Tunnel-List	O	27	Chaîne	Unique	Spécifie le nom du réseau ou de la liste de contrôle d'accès qui décrit la liste d'inclusion du tunnel fractionné.
IPsec-Tunnel-Type	O	30	nombre entier	Unique	1 = LAN à LAN 2 = Accès à distance
IPsec-User-Group-Lock		33	Booléen	Unique	0 = Désactivé 1 = Activé
IPv6-Address-Pools	O	218	Chaîne	Unique	Name of IP local pool-IPv6
IPv6-VPN-Filter	O	219	Chaîne	Unique	Valeur ACL
L2TP-Encryption		21	nombre entier	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 4 = 128 bits 8 = Stateless-Req 15 = 40/128-Encr/Stateless-Req
L2TP-MPPC-Compression		38	nombre entier	Unique	0 = Désactivé 1 = Activé

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Member-Of	O	145	Chaîne	Unique	Chaîne délimitée par des virgules, par exemple : `Engineering, Sales` Attribut administratif qui peut être utilisé dans les politiques d'accès dynamique. Elle ne définit pas de politique de groupe.
MS-Client-Subnet-Mask	O	63	Booléen	Unique	Une adresse IP
NAC-Default-ACL		92	Chaîne		ACL
NAC-Enable		89	nombre entier	Unique	0 = non 1 = oui
NAC-Revalidation-Timer		91	nombre entier	Unique	300 à 86 400 secondes
NAC-Settings	O	141	Chaîne	Unique	Nom de la politique NAC
NAC-Status-Query-Timer		90	nombre entier	Unique	30 à 1800 secondes
Perfect-Forward-Secrecy-Enable	O	88	Booléen	Unique	0 = non 1 = oui
PPTP-Encryption		20	nombre entier	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 4 = 128 bits 8 = Stateless-Requis 15= 40/128-Encr/Stateless-Req
PPTP-MPPC-Compression		37	nombre entier	Unique	0 = Désactivé 1 = Activé
Primary-DNS	O	5	Chaîne	Unique	Une adresse IP
Primary-WINS	O	7	Chaîne	Unique	Une adresse IP
Privilege-Level	O	220	nombre entier	Unique	Un nombre entier entre 0 et 15.
Required-Client-Firewall-Vendor-Code	O	45	nombre entier	Unique	1 = Cisco Systems (avec Cisco Integrated Client) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems (avecCisco Intrusion Prevention Security Agent)
Required-Client-Firewall-Description	O	47	Chaîne	Unique	Chaîne

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Required-Client-Firewall-Product Code	O	46	nombre entier	Unique	Produits Cisco Systems : 1 = Cisco Intrusion Prevention Security Agent ou Cisco Integrated Client (CIC) Produits Zone Labs : 1 = Alarme de zone 2 = Alarme de zone Pro 3 = Zone Labs Integrity Produit NetworkICE : 1 = NoirIce Defender/Agent Produits Sygate : 1 = Personal Firewall 2 = Personal Firewall Pro 3 = security Agent
Required-Individual-User-Auth	O	49	nombre entier	Unique	0 = Désactivé 1 = Activé
Require-HW-Client-Auth	O	48	Booléen	Unique	0 = Désactivé 1 = Activé
Secondary-DNS	O	6	Chaîne	Unique	Une adresse IP
Secondary-WINS	O	8	Chaîne	Unique	Une adresse IP
SEP-Card-Attribution		9	nombre entier	Unique	Non utilisé
Sous-type de session	O	152	nombre entier	Unique	0 = Aucun 1 = Sans client 2 = Client 3 = Client seulement Le sous-type de session s'applique uniquement lorsque l'attribut de type de session (151) a les valeurs suivantes : 1, 2, 3 et 4.
Type de séance	O	151	nombre entier	Unique	0 = Aucun 1 = Secure Client (services client sécurisés) VPN SSL 2 = Secure Client (services client sécurisés) VPN IPSec (IKEv2) 3 = VPN SSL sans client 4 = serveur mandataire de messagerie sans client 5 = Client Cisco VPN (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = Équilibrage de charge VPN
Connexions simultanées	O	2	nombre entier	Unique	0 à 2147483647
Smart-Tunnel	O	136	Chaîne	Unique	Nom d'un tunnel intelligent
Smart-Tunnel-Auto	O	138	nombre entier	Unique	0 = Désactivé 1 = Activé 2 = Démarrage automatique
Smart-Tunnel-Auto-Signon-Enable	O	139	Chaîne	Unique	Nom d'une liste de connexion automatique de tunnel Smart à côté du nom de domaine
Strip-Realm	O	135	Booléen	Unique	0 = Désactivé 1 = Activé
SVC-Ask	O	131	Chaîne	Unique	0 = Désactivé 1 = Activé 3 = Active le service par défaut 5 = Active l'absence de client par défaut (2 et 4 non utilisés)

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
SVC-Ask-Timeout	O	132	nombre entier	Unique	5 à 120 secondes
Client-SVC-DPD-Interval	O	108	nombre entier	Unique	0 = Désactivé, 5 à 3 600 secondes
Passerelle-SVC-DPD-Interval	O	109	nombre entier	Unique	0 = Désactivé) 5 à 3 600 secondes
SVC-DTLS	O	123	nombre entier	Unique	0 = faux 1 = vrai
SVC-Keepalive	O	107	nombre entier	Unique	0 = Désactivé, 15–600 secondes
SVC-Modules	O	127	Chaîne	Unique	Chaîne de caractères (nom d'un module)
SVC-MTU	O	125	nombre entier	Unique	Valeur MTU 256 à 1406 en octets
SVC-Profiles	O	128	Chaîne	Unique	Chaîne de caractères (nom d'un profil)
SVC-Rekey-Time	O	110	nombre entier	Unique	0 = Désactivé 1 à 10 080 minutes
Tunnel Group Name	O	146	Chaîne	Unique	1 à 253 caractères
Tunnel-Group-Lock	O	85	Chaîne	Unique	Nom du groupe de tunnels ou « none » (aucun)
Tunneling-Protocoles	O	11	nombre entier	Unique	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 et 4 s'excluent mutuellement. 0 à 11, 16 à 27, 32 à 43 et 48 à 59 sont des valeurs autorisées.
Use-Client-Address		17	Booléen	Unique	0 = Désactivé 1 = Activé
VLAN	O	140	nombre entier	Unique	0 à 4094
WebVPN-Access-List	O	73	Chaîne	Unique	Nom de la liste d'accès
WebVPN ACL	O	73	Chaîne	Unique	Nom d'une ACL WebVPN sur le périphérique
WebVPN-ActiveX-Relay	O	137	nombre entier	Unique	0 = Désactivé Sinon = Activé
WebVPN-Apply-ACL	O	102	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Auto-HTTP-Signon	O	124	Chaîne	Unique	Réservé
WebVPN-Citrix-Metaframe-Enable	O	101	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Content-Filter-Parameters	O	69	nombre entier	Unique	1 = Java ActiveX 2 = Java Script 4 = Image 8 = Témoins dans les images
WebVPN-Customization	O	113	Chaîne	Unique	Nom de la personnalisation
WebVPN-Default-Homepage	O	76	Chaîne	Unique	Une URL telle que http://exemple-exemple.com
WebVPN-Deny-Message	O	116	Chaîne	Unique	Chaîne de caractères valide (jusqu'à 500 caractères)

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-Download_Max-Size	O	157	nombre entier	Unique	0x7fffffff
WebVPN-File-Access-Enable	O	94	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Browsing-Enable	O	96	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Entry-Enable	O	95	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	O	78	Chaîne	Unique	DNS/IP séparés par des virgules avec un caractère générique facultatif (*) (par exemple *.cisco.com, 192.168.1.*, wwwin.cisco.com)
WebVPN-Hidden-Shares	O	126	nombre entier	Unique	0 = aucun 1 = visible
WebVPN-Home-Page-Use-Smart-Tunnel	O	228	Booléen	Unique	Activé si la page d'accueil sans client doit être affichée par l'intermédiaire de Smart Tunnel.
WebVPN-HTML-Filter	O	69	Bitmap	Unique	1 = ActiveX Java 2 = Scripts 4 = Image 8 = Témoins
WebVPN-HTTP-Compression	O	120	nombre entier	Unique	0 = Désactivé 1 = Décompression
WebVPN-HTTP-Proxy-IP-Address	O	74	Chaîne	Unique	DNS/IP séparé par des virgules:port, avec le préfixe http= ou https= (par exemple http=10.10.10:80, https=11.11.11.11:443)
WebVPN-Idle-Timeout-Alert-Interval	O	148	nombre entier	Unique	0 à 30. 0 = Désactivé.
WebVPN-Keepalive-Ignore	O	121	nombre entier	Unique	0 à 900
WebVPN-Macro-Substitution	O	223	Chaîne	Unique	Illimité.
WebVPN-Macro-Substitution	O	224	Chaîne	Unique	Illimité.
WebVPN-Port-Forwarding-Enable	O	97	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	O	98	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-HTTP-Proxy	O	99	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-List	O	72	Chaîne	Unique	Nom de la liste de transferts de port
WebVPN-Port-Forwarding-Name	O	79	Chaîne	Unique	Nom de chaîne de caractères (par exemple, « Corporate-Apps »). Ce texte remplace la chaîne par défaut « Application Access » dans la page d'accueil du portail sans client.
WebVPN-post-maximum-taille	O	159	nombre entier	Unique	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	O	149	nombre entier	Unique	0 à 30. 0 = Désactivé.

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN Smart-Card-Removal-Disconnect	O	225	Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-Smart-Tunnel	O	136	Chaîne	Unique	Nom d'un tunnel intelligent
WebVPN-Smart-Tunnel-Auto-Sign-On	O	139	Chaîne	Unique	Nom d'une liste de connexion automatique de Smart Tunnel ajouté par le nom de domaine
WebVPN-Smart-Tunnel-Auto-Start	O	138	nombre entier	Unique	0 = Désactivé 1 = Activé 2 = Démarrage automatique
WebVPN-Smart-Tunnel-Tunnel-Policy	O	227	Chaîne	Unique	Un des choix « e networkname », « i networkname » ou « a », où networkname est le nom d'une liste de réseaux Smart Tunnels, e indiquant le tunnel exclu, i le tunnel spécifié et a indique tous les tunnels.
WebVPN-SSL-VPN-Client-Enable	O	103	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSL-VPN-Client-Keep-Installation	O	105	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSL-VPN-Client-Required	O	104	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSO-Server-Name	O	114	Chaîne	Unique	Chaîne de caractères valide
WebVPN-Storage-Key	O	162	Chaîne	Unique	
WebVPN-Storage-Objects	O	161	Chaîne	Unique	
WebVPN-SVC-Keepalive-Frequency	O	107	nombre entier	Unique	15 à 600 secondes, 0 = désactivé
WebVPN-SVC-Client-DPD-Frequency	O	108	nombre entier	Unique	5 à 3 600 secondes, 0 = désactivé
WebVPN-SVC-DTLS-Enable	O	123	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SVC-DTLS-MTU	O	125	nombre entier	Unique	La valeur MTU est comprise entre 256 et 1406 octets.
WebVPN-SVC-Gateway-DPD-Frequency	O	109	nombre entier	Unique	5 à 3 600 secondes, 0 = désactivé
WebVPN-SVC-Rekey-Time	O	110	nombre entier	Unique	4 à 10 080 minutes, 0 = Désactivé
WebVPN-SVC-Rekey-Method	O	111	nombre entier	Unique	0 (désactivé), 1 (SSL), 2 (nouveau tunnel)
WebVPN-SVC-Compression	O	112	nombre entier	Unique	0 (Désactivé), 1 (Décompression)
WebVPN-UNIX-Group-ID (GID)	O	222	nombre entier	Unique	ID de groupe UNIX valides
WebVPN-UNIX-User-ID (UIDs)	O	221	nombre entier	Unique	ID d'utilisateur UNIX valides
WebVPN-Upload-Max-Size	O	158	nombre entier	Unique	0x7fffffff
WebVPN-URL-Entry-Enable	O	93	nombre entier	Unique	0 = Désactivé 1 = Activé

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-URL-List	O	71	Chaîne	Unique	Nom de la liste d'URL
WebVPN-User-Storage	O	160	Chaîne	Unique	
WebVPN-VDI	O	163	Chaîne	Unique	Liste des paramètres

Attributs d'autorisation RADIUS IETF pris en charge

Le tableau suivant présente les attributs RADIUS IETF pris en charge.

Tableau 50 : Attributs RADIUS IETF pris en charge

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IETF-Radius-Class	O	25		Unique	Pour les versions 8.2.x et ultérieures, nous vous recommandons d'utiliser l'attribut Group-Policy (VSA 3076, n° 25) : • *nom de la politique de groupe* • OU=*nom de la politique de groupe* • OU=*nom de la politique de groupe*
IETF-Radius-Filter-Id	O	11	Chaîne	Unique	Nom de l'ACL défini sur l'ASA, qui s'applique uniquement aux clients SSL VPN et IPsec du tunnel complet.
IETF-Radius-Framed-IP-Address	O	S.O.	Chaîne	Unique	Une adresse IP
IETF-Radius-Framed-IP-Netmask	O	S.O.	Chaîne	Unique	Un masque d'adresse IP
IETF-Radius-Idle-Timeout	O	28	nombre entier	Unique	Secondes
IETF-Radius-Service-Type	O	6	nombre entier	Unique	Secondes. Valeurs possibles pour le type de service : • .Administrative : l'utilisateur a accès à l'invite de configuration. • .NAS-Prompt : l'utilisateur a accès à l'invite d'exécution. • .remote-access : l'utilisateur a accès au réseau.
IETF-Radius-Session-Timeout	O	27	nombre entier	Unique	Secondes

Codes de motif de déconnexion comptable RADIUS

Ces codes sont renvoyés si l'ASA rencontre une déconnexion lors de l'envoi de paquets :

Code de motif de déconnexion
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

Lignes directrices relatives aux serveurs RADIUS pour AAA

Cette section décrit les lignes directrices et les limites que vous devez vérifier avant de configurer les serveurs RADIUS pour l'AAA.

- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 4 groupes de serveurs par contexte en mode multiple.
- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple.
- La longueur maximale de la charge utile RADIUS est de 4096 octets.

Configurer les serveurs RADIUS pour AAA

Cette section décrit comment configurer les serveurs RADIUS pour AAA.

Procédure

Étape 1 Chargez les attributs ASA dans le serveur RADIUS. La méthode que vous utilisez pour charger les attributs dépend du type de serveur RADIUS que vous utilisez :

- Si vous utilisez Cisco ACS : le serveur intègre déjà ces attributs. Vous pouvez ignorer cette étape.
- Pour les serveurs RADIUS d'autres fournisseurs (par exemple, le service d'authentification Internet Microsoft) : vous devez définir manuellement chaque attribut ASA. Pour définir un attribut, utilisez le nom ou le numéro d'attribut, le type, la valeur et le code du fournisseur (3076).

Étape 2 Configurer les groupes de serveurs RADIUS, à la page 1092.

Étape 3 Ajouter un serveur RADIUS à un groupe, à la page 1095.

Étape 4 (Facultatif) Ajouter une invite d'authentification, à la page 1097.

Configurer les groupes de serveurs RADIUS

Si vous souhaitez utiliser un serveur RADIUS externe pour l'authentification, l'autorisation ou la gestion de comptes, vous devez d'abord créer au moins un groupe de serveurs RADIUS par protocole AAA et ajouter un ou plusieurs serveurs à chaque groupe.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Cliquez sur **Add** (Ajouter) dans le champ **AAA Server Groups** (Groupes de serveurs AAA).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) apparaît.

Étape 3 Saisissez un nom pour le groupe dans le champ **AAA Server Group** (Groupe de serveurs AAA).

Étape 4 Dans la liste déroulante **Protocol** (Protocole), choisissez le type de serveur RADIUS.

Étape 5 Sélectionnez le **Accounting Mode** (Mode de comptabilité).

- **Simultaneous** (Simultané) : envoyez les données de gestion à tous les serveurs du groupe.

- **Single** (Unique) : envoyez les données de gestion à un seul serveur.

Étape 6 Configurez la méthode (**Reactivation Mode** (Mode de réactivation)) par laquelle les serveurs défaillants d'un groupe sont réactivés.

- **Depletion** (Épuisement), **Dead Time** (Temps mort) : réactivez les serveurs défaillants uniquement après que tous les serveurs du groupe sont inactifs. Il s'agit du mode de réactivation par défaut. Précisez la durée, entre 0 et 1 440 minutes, qui s'écoule entre la désactivation du dernier serveur du groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort. La valeur par défaut est 10 minutes.
- **Timed** (Temporisé) : réactivez les serveurs défaillants après 30 secondes de temps d'arrêt.

Étape 7 Dans **Max Failed Attempts** (Nombre max. de tentatives échouées), spécifiez le nombre maximum de transactions AAA échouées avec un serveur RADIUS du groupe avant d'essayer le serveur suivant.

La plage se situe entre 1 et 5. La valeur par défaut est de 3.

Si vous configurez une méthode de secours à l'aide de la base de données locale (pour l'accès de gestion uniquement), et que tous les serveurs du groupe ne répondent pas ou que leurs réponses ne sont pas valides, le groupe est considéré comme ne répondant pas et la méthode de secours est essayée. Le groupe de serveurs reste marqué comme ne répondant pas pendant une période de 10 minutes (si vous utilisez le mode de réactivation et le temps mort par défaut), de sorte que les demandes AAA supplémentaires effectuées dans cette période ne résultent pas en une tentative d'entrer en contact avec le groupe de serveurs et que la méthode de secours est utilisée immédiatement. Pour modifier la période de non-réponse par défaut, consultez la section qui explique comment modifier le **temps mort**.

Si vous n'avez pas de méthode de secours, l'ASA continue de réessayer les serveurs du groupe.

Étape 8 (Facultatif) Activez la génération périodique de messages RADIUS inter-accounting-update en sélectionnant les options souhaitées.

Ces options ne sont pertinentes que si vous utilisez ce groupe de serveurs pour Secure Client (services client sécurisés) ou le SSL VPN sans client.

- **Enable interim accounting update** (Activer la mise à jour de la comptabilité provisoire) : si vous utilisez cette commande sans sélectionner l'option **Update Interval** (Intervalle de mise à jour), l'ASA envoie des messages provisoires de comptabilité et de mise à jour uniquement lorsqu'une connexion de tunnel VPN est ajoutée à une session VPN sans client. Lorsque cela se produit, la mise à jour de comptabilité est générée afin d'informer le serveur RADIUS de la nouvelle adresse IP attribuée.
- **Update Interval** (Intervalle de mise à jour) : permet la génération et la transmission périodiques des enregistrements de comptabilité pour chaque session VPN configurée pour envoyer des enregistrements de comptabilité au groupe de serveurs en question. Vous pouvez modifier l'intervalle, en heures, pour l'envoi de ces mises à jour. La valeur par défaut est de 24 heures, la plage est comprise entre 1 et 120.



Remarque Pour les groupes de serveurs contenant des serveurs ISE, sélectionnez les deux options. ISE gère un répertoire des sessions actives en fonction des enregistrements de traçabilité qu'il reçoit des périphériques NAS comme l'ASA. Cependant, si ISE ne reçoit aucune indication que la session est toujours active (message de traçabilité ou transactions de posture) pendant une période de 5 jours, il supprimera l'enregistrement de session de sa base de données. Pour vous assurer que les connexions VPN de longue durée ne sont pas supprimées, configurez le groupe pour envoyer des messages interim-accounting-update périodiques à ISE pour toutes les sessions actives.

Étape 9 (Facultatif) Si ce groupe contient uniquement des serveurs d'agents AD ou d'agents Cisco Directory (CDA), sélectionnez **Enable Active Directory Agent Mode** (Activer le mode agent Active Directory).

Les agents CDA ou AD sont utilisés dans le pare-feu d'identité et ne sont pas des serveurs RADIUS complets. Si vous sélectionnez cette option, vous pouvez utiliser ce groupe à des fins de pare-feu d'identité uniquement.

Étape 10 (Facultatif) Si vous utilisez ce groupe de serveurs pour l'application de la politique ISE dans le VPN d'accès à distance, configurez les options suivantes :

- **Enable dynamic authorization** (Activer l'autorisation dynamique) : active les services d'autorisation dynamique ou de changement d'autorisation (CoA) RADIUS pour ce groupe de serveurs RADIUS. Lorsque vous utilisez le groupe de serveurs dans un tunnel VPN, le groupe de serveurs RADIUS sera enregistré pour la notification CoA et l'ASA écoutera le port pour détecter les mises à jour de politique CoA d'ISE. Activez l'autorisation dynamique uniquement si vous utilisez ce groupe de serveurs dans un VPN d'accès à distance en conjonction avec l'ISE.
- **Dynamic Authorization Port** (Port d'autorisation dynamique) : si vous activez l'autorisation dynamique, vous pouvez spécifier le port d'écoute pour les demandes RADIUS CoA. La valeur par défaut est 1700. La plage valide est de 1024 à 65535.
- **Use authorization only mode** (Utiliser le mode d'autorisation uniquement) : si vous ne souhaitez pas utiliser ISE pour l'authentification, activez le mode d'autorisation uniquement pour le groupe de serveurs RADIUS. Cela indique que lorsque ce groupe de serveurs est utilisé pour l'autorisation, le message de demande d'accès RADIUS sera généré en tant que demande « Autorize Only » (Autorisation uniquement), par opposition aux méthodes de mot de passe configurées pour le serveur AAA. Si vous configurez un mot de passe commun pour le serveur RADIUS, il sera ignoré.

  Par exemple, vous utiliserez le mode d'autorisation seulement si vous souhaitez utiliser des certificats pour l'authentification plutôt que ce groupe de serveurs. Vous utiliserez toujours ce groupe de serveurs pour l'autorisation et la gestion de comptes dans le tunnel VPN.

Étape 11 (Facultatif) Configurez le champ **VPN3K Compatibility Option** (Option de compatibilité VPN3K) pour spécifier si une ACL téléchargeable reçue d'un paquet RADIUS doit être fusionnée ou non avec une ACL de paire attribut/valeur de Cisco.

Cette option s'applique uniquement aux connexions VPN. Pour les utilisateurs de VPN, les ACL peuvent prendre la forme d'ACL de paire attribut/valeur de Cisco, d'ACL téléchargeables et d'une ACL configurée sur l'ASA. Cette option détermine si l'ACL téléchargeable et l'ACL de la paire attribut/valeur sont fusionnées, et ne s'applique à aucune ACL configurée sur l'ASA.

- **Do not merge** (Ne pas fusionner) : les ACL téléchargeables ne seront pas fusionnées avec les ACL de paire AV de Cisco. Si une paire AV et une ACL téléchargeable sont reçues, la paire AV a la priorité et est utilisée. Il s'agit de l'option par défaut.

- **Placez l'ACL téléchargeable après l'ACL de la paire AV de Cisco**
- **Placez l'ACL téléchargeable avant l'ACL de la paire AV de Cisco**

Étape 12 Cliquez sur **OK**.

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) se ferme et le nouveau groupe de serveurs est ajouté au tableau **AAA Server Groups** (Groupes de serveurs AAA).

Étape 13 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Ajouter un serveur RADIUS à un groupe

Pour ajouter un serveur RADIUS à un groupe, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**, et dans la zone **AAA Server Groups** (Groupes de serveurs AAA), cliquez sur le groupe de serveurs auquel vous souhaitez ajouter un serveur.

Étape 2 Cliquez sur **Add** (Ajouter) dans la zone **Servers in the Selected Group** (Serveurs du groupe sélectionné) (volet inférieur).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) s'affiche pour le groupe de serveurs.

Étape 3 Choisissez le nom de l'interface sur laquelle se trouve le serveur d'authentification.

Étape 4 Ajoutez un nom de serveur ou une adresse IP pour le serveur que vous ajoutez au groupe.

Étape 5 Spécifiez la valeur du délai d'expiration pour les tentatives de connexion au serveur.

Spécifiez l'intervalle du délai d'expiration (1 à 300 secondes) du serveur; la valeur par défaut est de 10 secondes. Pour chaque transaction AAA, l'ASA relance les tentatives de connexion (en fonction de l'intervalle de nouvelle tentative) jusqu'à ce que le délai d'expiration soit atteint. Si le nombre de transactions consécutives ayant échoué atteint la limite maximum-failed-attempts spécifiée dans le groupe de serveurs AAA, le serveur AAA est désactivé et l'ASA commence à envoyer des demandes à un autre serveur AAA s'il est configuré.

Étape 6 Spécifiez comment vous souhaitez que l'ASA gère les masques réseau reçus dans les ACL téléchargeables. Choisissez parmi les options suivantes :

- **Detect automatically** (Détecter automatiquement) : l'ASA tente de déterminer le type d'expression de masque réseau utilisé. Si l'ASA détecte une expression de masque réseau à caractère générique, l'ASA la convertit en une expression de masque réseau standard.

Remarque Étant donné que certaines expressions à caractère générique sont difficiles à détecter clairement, ce paramètre peut interpréter de manière erronée une expression de masque réseau à caractère générique comme une expression de masque réseau standard.

- **Standard** : l'ASA suppose que les ACL téléchargeables reçues du serveur RADIUS contiennent uniquement des expressions de masque réseau standard. Aucune conversion des expressions de masque réseau à caractère générique n'est effectuée.
- **Générique** : l'ASA suppose que les ACL téléchargeables reçues du serveur RADIUS contiennent uniquement des expressions de masque réseau à caractère générique et les convertit toutes en des expressions de masque réseau standard lorsque les ACL sont téléchargées.

Étape 7 Spécifiez un mot de passe sensible à la casse commun aux utilisateurs qui accèdent à ce serveur d'autorisation RADIUS par l'intermédiaire de cet ASA. Assurez-vous de fournir ces renseignements à l'administrateur de votre serveur RADIUS.

Remarque Pour un serveur RADIUS d'authentification (plutôt que d'autorisation), ne configurez pas de mot de passe commun.

Si vous laissez ce champ vide, le nom d'utilisateur devient le mot de passe pour accéder à ce serveur d'autorisation RADIUS.

N'utilisez jamais un serveur d'autorisation RADIUS pour l'authentification. Les mots de passe ou noms d'utilisateur communs sont moins sécurisés que l'attribution de mots de passe d'utilisateur uniques.

Bien que le mot de passe soit requis par le protocole RADIUS et le serveur RADIUS, les utilisateurs n'ont pas besoin de le connaître.

Étape 8 Si vous utilisez la double authentification et activez la gestion des mots de passe dans le groupe de tunnels, les demandes d'authentification principale et secondaire incluent les attributs de demande MS-CHAPv2. Si un serveur RADIUS ne prend pas en charge MS-CHAPv2, vous pouvez configurer ce serveur pour envoyer une demande d'authentification non MS-CHAPv2 en décochant cette case.

Étape 9 Précisez la durée, de 1 à 10 secondes, pendant laquelle l'ASA attend entre deux tentatives de connexion au serveur.

Remarque Pour le protocole RADIUS, si le serveur répond par un message de port ICMP inaccessible, le paramètre retry-interval est ignoré et le serveur AAA passe immédiatement à l'état d'échec. S'il s'agit du seul serveur du groupe AAA, il est réactivé et une autre requête lui est envoyée. Il s'agi du comportement prévu.

Étape 10 Cliquez sur **Simultaneous** (Simultané) ou **Single** (Unique).

En mode unique, l'ASA envoie des données comptables à un seul serveur.

En mode simultané, l'ASA envoie des données comptables à tous les serveurs du groupe.

Étape 11 Précisez le port de serveur à utiliser pour la comptabilisation des utilisateurs. La valeur du port par défaut est 1646.

Étape 12 Précisez le port de serveur à utiliser pour l'authentification des utilisateurs. La valeur du port par défaut est 1645.

Étape 13 Spécifiez la clé secrète partagée utilisée pour authentifier le serveur RADIUS auprès de l'ASA. La clé du serveur que vous configurez doit correspondre à celle configurée sur le serveur RADIUS. Si vous ne connaissez pas la clé secrète du serveur, demandez à l'administrateur du serveur RADIUS. La longueur maximale du champ est de 64 caractères.

Étape 14 Cliquez sur **OK**.

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) se ferme et le serveur AAA est ajouté au groupe de serveurs AAA.

Étape 15 Dans le volet **AAA Server Groups** (Groupes de serveurs AAA), cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Ajouter une invite d'authentification

Vous pouvez spécifier le texte de défi AAA pour l'accès HTTP, FTP et Telnet par l'intermédiaire de l'ASA lors de la demande d'authentification de l'utilisateur sur les serveurs RADIUS. Ce texte est principalement cosmétique et apparaît au-dessus des invites de nom d'utilisateur et de mot de passe que les utilisateurs voient lorsqu'ils se connectent. Si vous ne spécifiez pas d'invite d'authentification, les utilisateurs verront les éléments suivants lorsqu'ils s'authentifient auprès d'un serveur RADIUS :

Type de connexion	Invite par défaut
FTP	Authentification FTP
HTTP	Authentification HTTP
Telnet	Aucune

Pour ajouter une invite d'authentification, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Authentication Prompt (Invite d'authentification)**.

Étape 2 Saisissez du texte dans le champ **Prompt** (Invite) pour ajouter un message afin qu'il s'affiche au-dessus des invites de nom d'utilisateur et de mot de passe que les utilisateurs voient lorsqu'ils se connectent.

Le tableau suivant affiche les limites de caractères autorisées pour les invites d'authentification :

Application	Limite de caractères
Microsoft Internet Explorer	37
Telnet	235

Application	Limite de caractères
FTP	235

Étape 3 Ajoutez des messages dans les champs **User accepted message** (Message accepté par l'utilisateur) et **User rejected message** (Message refusé par l'utilisateur).

Si l'authentification de l'utilisateur a lieu à partir de Telnet, vous pouvez utiliser les options **User accepted message** (Message accepté par l'utilisateur) et **User rejected message** (Message refusé par l'utilisateur) pour afficher différents états afin d'indiquer que la tentative d'authentification est acceptée ou refusée par le serveur RADIUS.

Si le serveur RADIUS authentifie l'utilisateur, l'ASA affiche le texte **User accepted message** (Message accepté par l'utilisateur), si spécifié, à l'utilisateur; sinon, l'ASA affiche le texte **User rejected message** (Message refusé par l'utilisateur), si cela est spécifié. L'authentification des sessions HTTP et FTP affiche uniquement le texte de défi à l'invite. Le texte des **messages acceptés** ou **refusés par l'utilisateur** ne s'affiche pas.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Tester l'authentification et l'autorisation du serveur RADIUS

Pour déterminer si l'ASA peut communiquer avec un serveur RADIUS et authentifier ou autoriser un utilisateur, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Cliquez sur le groupe de serveurs dans lequel se trouve le serveur dans le tableau **AAA Server Groups** (Groupes de serveurs AAA).

Étape 3 Cliquez sur le serveur que vous souhaitez tester dans le tableau **Servers in the Selected Group** (Serveurs du groupe sélectionné).

Étape 4 Cliquez sur **Test**.

La boîte de dialogue **Test AAA Server** (Tester un serveur AAA) s'affiche pour le groupe de serveurs sélectionné.

Étape 5 Cliquez sur le type de test que vous souhaitez effectuer : **Authentication** (Authentification) ou **Authorization** (Autorisation).

Étape 6 Saisissez un nom d'utilisateur.

Étape 7 Saisissez le mot de passe pour le nom d'utilisateur si vous testez l'authentification.

Étape 8 Cliquez sur **OK**.

L'ASA envoie un message de test d'authentification ou d'autorisation au serveur. Si le test échoue, un message d'erreur s'affiche.

Supervision des serveurs RADIUS pour AAA

Consultez les commandes suivantes pour superviser l'état des serveurs RADIUS pour AAA :

- **Monitoring (Supervision) > Properties (Propriétés) > AAA Servers (Serveurs AAA)**

  Ce volet montre la configuration d'exécution du serveur RADIUS.

- **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

Historique des serveurs RADIUS pour AAA

Tableau 51 : Historique des serveurs RADIUS pour AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs RADIUS pour AAA	7.0(1)	Décrit comment configurer les serveurs RADIUS pour AAA. Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Server Groups Configuration (Configuration des groupes de serveurs AAA) > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > Authentication Prompt (Invite d'authentification).
Attributs propres au fournisseur de clé (VSA) envoyés dans les paquets de demande d'accès et de demande de comptabilité RADIUS à partir de l'ASA	8.4(3)	Quatre nouveaux VSA : le nom du groupe de tunnels (146) et le type de client (150) sont envoyés dans les paquets de demande d'accès RADIUS à partir de l'ASA. Le type de session (151) et le sous-type de session (152) sont envoyés dans les paquets de demande de comptabilité RADIUS à partir de l'ASA. Les quatre attributs sont envoyés pour tous les types de paquets de demande de comptabilité : Start, Interim-Update et Stop. Le serveur RADIUS (par exemple, ACS et ISE) peut alors appliquer des attributs d'autorisation et de politique ou les utiliser à des fins de comptabilité et de facturation.

Nom de la caractéristique	Versions de plateforme	Description
Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe.	9.13(1)	Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4). En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée. Nous avons modifié les écrans AAA pour accepter ces nouvelles limites.



CHAPITRE 40

Serveurs TACACS+ pour AAA

Ce chapitre décrit comment configurer les serveurs TACACS+ utilisés dans AAA.

- À propos des serveurs TACACS+ pour AAA, à la page 1101
- Lignes directrices relatives aux serveurs TACACS+ pour AAA, à la page 1103
- Configurer les serveurs TACACS+, à la page 1103
- Tester l'authentification et l'autorisation des serveurs TACACS+, à la page 1106
- Supervision des serveurs TACACS+ pour AAA, à la page 1107
- Historique des serveurs TACACS+ pour AAA, à la page 1108

À propos des serveurs TACACS+ pour AAA

L'ASA prend en charge l'authentification du serveur TACACS+ avec les protocoles suivants : ASCII, PAP, CHAP et MS-CHAPv1.

Attributs TACACS+

L'ASA prend en charge les attributs TACACS+. Les attributs TACACS+ séparent les fonctions d'authentification, d'autorisation et de gestion de comptes. Le protocole prend en charge deux types d'attributs : obligatoires et facultatifs. Le serveur et le client doivent comprendre un attribut obligatoire, et l'attribut obligatoire doit être appliqué à l'utilisateur. Un attribut facultatif peut ne pas être compris ou utilisé.

Remarque Pour utiliser les attributs TACACS+, assurez-vous d'avoir activé les services AAA sur le NAS.

Le tableau suivant répertorie les attributs de réponse d'autorisation TACACS+ pris en charge pour les connexions de mandataire direct.

Tableau 52 : Attributs de réponse d'autorisation TACACS+ pris en charge

Attribut	Description
acl	Identifie une ACL configurée localement à appliquer à la connexion.
idletime	Indique la durée d'inactivité en minutes qui est autorisée avant la fin de la session de l'utilisateur authentifié.

Attribut	Description
timeout	Spécifie la durée absolue en minutes pendant laquelle les informations d'authentification restent actives avant la fin de la session de l'utilisateur authentifié.

Le tableau suivant répertorie les attributs de comptabilité TACACS+ pris en charge.

.

Tableau 53 : Attributs de comptabilité TACACS+ pris en charge

Attribut	Description
bytes_in	Spécifie le nombre d'octets d'entrée transférés lors de cette connexion (enregistrements d'arrêt uniquement).
bytes_out	Spécifie le nombre d'octets de sortie transférés lors de cette connexion (enregistrements d'arrêt uniquement).
CMD	Définit la commande exécutée (comptabilisation des commandes uniquement).
disc-cause	Indique le code numérique qui identifie la raison de la déconnexion (enregistrements d'arrêt uniquement).
elapsed_time	Définit le temps écoulé en secondes pour la connexion (enregistrements d'arrêt uniquement).
foreign_ip	Indique l'adresse IP du client pour les connexions du tunnel. Définit l'adresse sur l'interface de sécurité la plus basse pour les connexions de mandataire direct.
local_ip	Spécifie l'adresse IP à laquelle le client s'est connecté pour les connexions du tunnel. Définit l'adresse sur l'interface de sécurité la plus élevée pour les connexions de mandataire direct.
Port NAS	Contient un ID de session pour la connexion.
packs_in	Indique le nombre de paquets d'entrée transférés lors de cette connexion.
packs_out	Indique le nombre de paquets de sortie transférés lors de cette connexion.
priv-level	Définit le niveau de privilège de l'utilisateur pour les demandes de comptabilité des commandes ou 1 dans le cas contraire.
rem_iddr	Indique l'adresse IP du client.
service	Spécifie le service utilisé. Toujours défini sur « shell » pour la comptabilisation des commandes uniquement.
task_id	Spécifie un ID de tâche unique pour la transaction de comptabilité.
nom d'utilisateur	Indique le nom de l'utilisateur.

Lignes directrices relatives aux serveurs TACACS+ pour AAA

Cette section décrit les lignes directrices et les limites que vous devez vérifier avant de configurer les serveurs TACACS+ pour l'AAA.

IPv6

Le serveur AAA peut utiliser une adresse IPv4 ou IPv6.

Directives supplémentaires

- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 4 groupes de serveurs par contexte en mode multiple.
- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple.
- Si vous configurez l'authentification à plusieurs facteurs avec ISE TACACS+ et Duo, vous devrez peut-être saisir à nouveau votre mot de passe lorsque vous établirez des connexions SSH après avoir confirmé la connexion avec Duo.
- Pour la série FPR1000, FPR2100 ou FPR3100 qui s'exécute sur l'ASA en mode appareil, vous devez vous conformer à ces conventions de nom d'utilisateur :
  - Les noms d'utilisateur doivent être valides sous Linux.
  - Ils doivent être uniquement en minuscules.
  - Ils peuvent inclure des caractères alphanumériques, des points (.) ou des tirets (-).
  - Ils ne doivent pas inclure d'autres caractères spéciaux tels que l'arobase (@) et la barre oblique (/).

Configurer les serveurs TACACS+

Cette section décrit comment configurer les serveurs TACACS+.

Procédure

Étape 1 Configurer les groupes de serveurs TACACS+, à la page 1103.

Étape 2 Ajouter un serveur TACACS+ à un groupe, à la page 1104.

Étape 3 (Facultatif) Ajouter une invite d'authentification, à la page 1105

Configurer les groupes de serveurs TACACS+

Si vous souhaitez utiliser un serveur TACACS+ pour l'authentification, l'autorisation ou la gestion de comptes, vous devez d'abord créer au moins un groupe de serveurs TACACS+ et ajouter un ou plusieurs serveurs à chaque groupe. Vous identifiez les groupes de serveurs TACACS+ par leur nom.

Pour ajouter un groupe de serveurs TACACS+, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Cliquez sur **Add** (Ajouter) dans le champ **AAA Server Groups** (Groupes de serveurs AAA).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) apparaît.

Étape 3 Saisissez un nom pour le groupe dans le champ **Server Group** (Groupe de serveurs).

Étape 4 Dans la liste déroulante **Protocol** (Protocole), choisissez le type de serveur **TACACS+** :

Étape 5 Cliquez sur **Simultaneous** ou **Single (Single)** dans le champ **Accounting Mode (Mode de comptabilité)**.

En mode unique, l'ASA envoie des données comptables à un seul serveur.

En mode simultané, l'ASA envoie des données comptables à tous les serveurs du groupe.

Étape 6 Cliquez sur **Depletion** (Épuisement) ou **Timed** (Temporisé) dans le champ **Reactivation Mode** (Mode de réactivation).

En mode Depletion (Épuisement), les serveurs défaillants ne sont réactivés qu'une fois que tous les serveurs du groupe sont inactifs. En mode d'épuisement, lorsqu'un serveur est désactivé, il reste inactif jusqu'à ce que tous les autres serveurs du groupe soient inactifs. Lorsque et si cela se produit, tous les serveurs du groupe sont réactivés. Cette approche réduit le nombre de retards de connexion en raison de serveurs défaillants.

En mode Timed (Temporisé), les serveurs défaillants sont réactivés après 30 secondes de temps d'arrêt.

Étape 7 Si vous avez choisi le mode de réactivation Depletion (Épuisement), saisissez un intervalle de temps dans le champ **Dead Time** (Temps mort).

Le temps mort est la durée, en minutes, qui s'écoule entre la désactivation du dernier serveur d'un groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort.

Étape 8 Ajoutez le nombre maximum de transactions AAA échouées avec un serveur à autoriser.

Cette option définit le nombre de transactions AAA ayant échoué avant de déclarer inactif un serveur qui ne répond pas.

Étape 9 Cliquez sur **OK**.

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) se ferme et le nouveau groupe de serveurs est ajouté au tableau **AAA Server Groups** (Groupes de serveurs AAA).

Étape 10 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Ajouter un serveur TACACS+ à un groupe

Pour ajouter un serveur TACACS+ à un groupe, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Cliquez sur le groupe de serveurs auquel vous souhaitez ajouter un serveur.

Étape 3 Cliquez sur **Add** (Ajouter) dans la zone **Servers in the Selected Group** (Serveurs du groupe sélectionné).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) s'affiche pour le groupe de serveurs.

Étape 4 Choisissez le nom de l'interface sur laquelle se trouve le serveur d'authentification.

Étape 5 Ajoutez un nom de serveur ou une adresse IP pour le serveur que vous ajoutez au groupe.

Étape 6 Spécifiez la valeur du délai d'expiration pour les tentatives de connexion au serveur.

Spécifiez l'intervalle du délai d'expiration (1 à 300 secondes) du serveur; la valeur par défaut est de 10 secondes. Pour chaque transaction AAA, l'ASA relance les tentatives de connexion (en fonction de l'intervalle de nouvelle tentative) jusqu'à ce que le délai d'expiration soit atteint. Si le nombre de transactions consécutives ayant échoué atteint la limite maximum-failed-attempts spécifiée dans le groupe de serveurs AAA, le serveur AAA est désactivé et l'ASA commence à envoyer des demandes à un autre serveur AAA s'il est configuré.

Étape 7 Spécifiez le Server Port (Port du serveur). Le port du serveur est le numéro de port 139 ou le numéro de port TCP utilisé par l'ASA pour communiquer avec le serveur TACACS+.

Étape 8 Spécifiez la clé secrète du serveur. La clé secrète partagée utilisée pour authentifier le serveur TACACS+ auprès de l'ASA. La clé secrète du serveur que vous configurez ici doit correspondre à celle configurée sur le serveur TACACS+. Si vous ne connaissez pas la clé secrète du serveur, demandez à l'administrateur du serveur TACACS+. La longueur maximale du champ est de 64 caractères.

Étape 9 Cliquez sur **OK**.

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) se ferme et le serveur AAA est ajouté au groupe de serveurs AAA.

Étape 10 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Ajouter une invite d'authentification

Vous pouvez spécifier le texte à afficher à l'utilisateur pendant le processus de défi d'authentification AAA. Vous pouvez spécifier le texte de défi AAA pour l'accès HTTP, FTP et Telnet par l'intermédiaire de l'ASA lors de la demande d'authentification de l'utilisateur sur les serveurs TACACS+. Ce texte est principalement cosmétique et apparaît au-dessus des invites de nom d'utilisateur et de mot de passe que les utilisateurs voient lorsqu'ils se connectent.

Si vous ne spécifiez pas d'invite d'authentification, les utilisateurs voient les éléments suivants lorsqu'ils s'authentifient auprès d'un serveur TACACS+ :

Type de connexion	Invite par défaut
FTP	Authentification FTP

Type de connexion	Invite par défaut
HTTP	Authentification HTTP
Telnet	Aucune

Pour ajouter une invite d'authentification, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Authentication Prompt (Invite d'authentification)**.

Étape 2 Ajoutez du texte pour qu'il s'affiche au-dessus des invites de nom d'utilisateur et de mot de passe que les utilisateurs voient lorsqu'ils se connectent.

Le tableau suivant affiche les limites de caractères autorisées pour les invites d'authentification :

Application	Limite de caractères pour l'invite d'authentification
Microsoft Internet Explorer	37
Telnet	235.
FTP	235.

Étape 3 Ajoutez des messages dans les champs **User accepted message** (Message accepté par l'utilisateur) et **User rejected message** (Message refusé par l'utilisateur).

Si l'authentification de l'utilisateur a lieu à partir de Telnet, vous pouvez utiliser les options **User accepted message** (Message accepté par l'utilisateur) et **User rejected message** (Message refusé par l'utilisateur) pour afficher différents états afin d'indiquer que la tentative d'authentification est acceptée ou refusée par le serveur AAA.

Si le serveur AAA authentifie l'utilisateur, l'ASA affiche le texte **User accepted message** (Message accepté par l'utilisateur), si spécifié, à l'utilisateur; sinon, l'ASA affiche le texte **User rejected message** (Message refusé par l'utilisateur), si cela est spécifié. L'authentification des sessions HTTP et FTP affiche uniquement le texte de défi à l'invite. Le texte des messages acceptés ou refusés par l'utilisateur ne s'affiche pas.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Tester l'authentification et l'autorisation des serveurs TACACS+

Pour déterminer si l'ASA peut communiquer avec un serveur TACACS+ et authentifier ou autoriser un utilisateur, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Cliquez sur le groupe de serveurs dans lequel se trouve le serveur.

Étape 3 Cliquez sur le serveur que vous souhaitez tester.

Étape 4 Cliquez sur **Test**.

La boîte de dialogue **Test AAA Server** (Tester un serveur AAA) s'affiche pour le groupe de serveurs sélectionné.

Étape 5 Cliquez sur le type de test que vous souhaitez effectuer : **Authentication** (Authentification) ou **Authorization** (Autorisation).

Étape 6 Saisissez un nom d'utilisateur.

Étape 7 Si vous testez l'authentification, saisissez le mot de passe correspondant au nom d'utilisateur.

Étape 8 Cliquez sur **OK**.

L'ASA envoie un message de test d'authentification ou d'autorisation au serveur. Si le test échoue, un message d'erreur s'affiche.

Supervision des serveurs TACACS+ pour AAA

Consultez les commandes suivantes pour superviser les serveurs TACACS+ pour AAA :

- **Monitoring (Supervision) > Properties (Propriétés) > AAA Servers (Serveurs AAA)**

  Ce volet affiche les statistiques du serveur TACACS+ configuré.

- **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

Historique des serveurs TACACS+ pour AAA

Tableau 54 : Historique des serveurs TACACS+ pour AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs TACACS+	7.0(1)	Décrit comment configurer les serveurs TACACS+ pour AAA. Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Server Groups (Groupes de serveurs AAA) Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > Authentication Prompt (Invite d'authentification)
Serveurs TACACS+ avec adresses IPv6 pour AAA	9.7(1)	Vous pouvez maintenant utiliser une adresse IPv4 ou IPv6 pour le serveur AAA.
Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe.	9.13(1)	Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4). En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée. Nous avons modifié les écrans AAA pour accepter ces nouvelles limites.



CHAPITRE 41

Serveurs LDAP pour AAA

Ce chapitre décrit comment configurer les serveurs LDAP utilisés dans AAA.

- À propos de LDAP et de l'ASA, à la page 1109
- Lignes directrices relatives aux serveurs LDAP pour AAA, à la page 1113
- Configurer les serveurs LDAP pour AAA, à la page 1114
- Tester l'authentification et l'autorisation du serveur LDAP, à la page 1118
- Supervision des serveurs LDAP pour AAA, à la page 1118
- Historique des serveurs LDAP pour AAA, à la page 1119

À propos de LDAP et de l'ASA

L'ASA est compatible avec la plupart des serveurs de répertoire LDAPv3, notamment :

- Sun Microsystems JAVA System Directory Server, fait désormais partie de l'édition Enterprise du serveur de répertoire Oracle, et anciennement nommé serveur de répertoire Sun ONE
- Microsoft Active Directory
- Novell
- OpenLDAP

Par défaut, l'ASA détecte automatiquement s'il est connecté à Microsoft Active Directory, Sun LDAP, Novell, OpenLDAP ou à un serveur de répertoire LDAPv3 générique. Toutefois, si la détection automatique ne parvient pas à déterminer le type de serveur LDAP, vous pouvez le configurer manuellement.

Fonctionnement de l'authentification avec LDAP

Pendant l'authentification, l'ASA agit comme mandataire client auprès du serveur LDAP pour l'utilisateur et s'authentifie auprès du serveur LDAP en texte brut ou à l'aide du protocole SASL. Par défaut, l'ASA transmet les paramètres d'authentification, généralement un nom d'utilisateur et un mot de passe, au serveur LDAP en texte brut.

L'ASA prend en charge les mécanismes SASL suivants, répertoriés par ordre croissant de puissance :

- Digest-MD5 : l'ASA répond au serveur LDAP par une valeur MD5 calculée à partir du nom d'utilisateur et du mot de passe.

- Kerberos : l'ASA répond au serveur LDAP en envoyant le nom d'utilisateur et le domaine à l'aide du mécanisme GSSAPI Kerberos.

L'ASA et le serveur LDAP prennent en charge toutes les combinaisons possibles de ces mécanismes SASL. Si vous configurez plusieurs mécanismes, l'ASA récupère la liste des mécanismes SASL configurés sur le serveur et définit le mécanisme d'authentification le plus puissant configuré à la fois sur l'ASA et le serveur. Par exemple, si le serveur LDAP et l'ASA prennent en charge les deux mécanismes, l'ASA sélectionne Kerberos, le plus fort des deux.

Une fois l'authentification LDAP de l'utilisateur réussie, le serveur LDAP renvoie les attributs pour l'utilisateur authentifié. Pour l'authentification VPN, ces attributs incluent généralement des données d'autorisation appliquées à la session VPN. Dans ce cas, l'utilisation de LDAP permet d'effectuer l'authentification et l'autorisation en une seule étape.

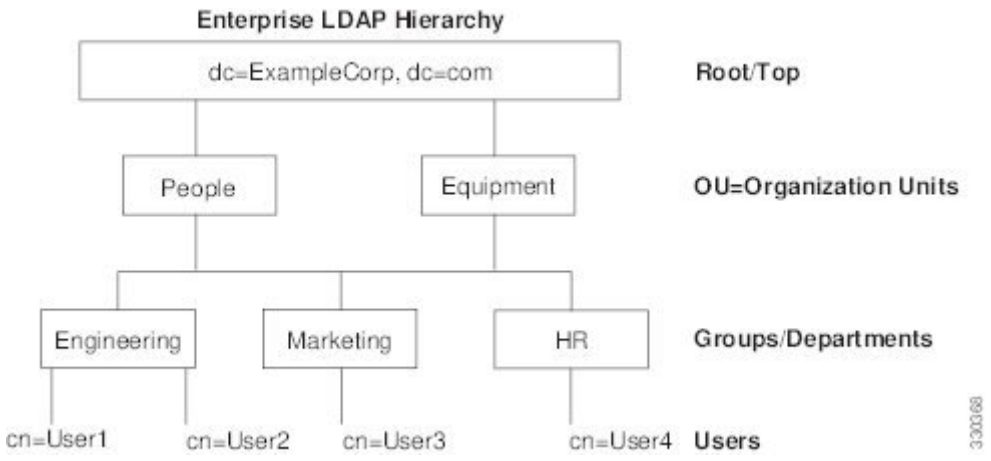
Remarque Pour en savoir plus sur LDAP, consultez les RFC 1777, 2251 et 2849.

Hiérarchie LDAP

Votre configuration LDAP doit refléter la hiérarchie logique de votre organisation. Par exemple, supposons qu'un employé de votre entreprise, Exemple Société, s'intitule Employé1. Employé 1 travaille dans le groupe d'ingénierie. Votre hiérarchie LDAP peut comporter un ou plusieurs niveaux. Vous pourriez décider de configurer une hiérarchie à un seul niveau dans laquelle Employé1 est considéré comme membre d'Exemple Société. Ou vous pouvez configurer une hiérarchie à plusieurs niveaux dans laquelle Employé1 est considéré comme un membre du service d'ingénierie, qui est lui-même membre d'une unité organisationnelle appelée Personnel, qui est elle-même membre d'Exemple Société. Consultez la figure suivante pour obtenir un exemple de hiérarchie à plusieurs niveaux.

Une hiérarchie à plusieurs niveaux est plus détaillée, mais les recherches renvoient des résultats plus rapidement dans une hiérarchie à un seul niveau.

Illustration 88 : Une hiérarchie LDAP à plusieurs niveaux



Rechercher dans la hiérarchie LDAP

L'ASA vous permet d'adapter la recherche dans la hiérarchie LDAP. Vous devez configurer les trois champs suivants sur l'ASA pour définir à quel niveau de la hiérarchie LDAP votre recherche doit commencer, son étendue et le type de renseignements que vous recherchez. Ensemble, ces champs limitent la recherche dans la hiérarchie à la partie qui inclut les autorisations des utilisateurs.

- Le DN de base LDAP définit à quel niveau de la hiérarchie LDAP le serveur doit commencer à rechercher les renseignements de l'utilisateur lorsqu'il reçoit une demande d'autorisation de l'ASA.
- La portée de recherche définit l'étendue de la recherche dans la hiérarchie LDAP. La recherche se poursuit sur ces nombreux niveaux dans la hiérarchie sous le DN de base LDAP. Vous pouvez choisir de demander au serveur de rechercher uniquement le niveau immédiatement en dessous, ou il peut rechercher dans toute la sous-arborescence. Une recherche à un seul niveau est plus rapide, mais une recherche dans la sous-arborescence est plus approfondie.
- Les attributs de nommage définissent le RDN qui identifie de manière unique une entrée dans le serveur LDAP. Les attributs de nommage courants peuvent inclure cn (nom commun), sAMAccountName et userPrincipalName.

La figure montre un exemple de hiérarchie LDAP pour l'exemple de société. Compte tenu de cette hiérarchie, vous pouvez définir votre recherche de différentes manières. Le tableau suivant présente deux exemples de configuration de recherche.

Dans le premier exemple de configuration, lorsque Employé1 établit le tunnel IPsec avec l'autorisation LDAP requise, l'ASA envoie une demande de recherche au serveur LDAP, indiquant qu'il doit rechercher Employé1 dans le groupe d'ingénierie. Cette recherche est rapide.

Dans le deuxième exemple de configuration, l'ASA envoie une demande de recherche indiquant que le serveur doit rechercher Employé1 dans l'exemple de société. Cette recherche prend plus de temps.

Tableau 55 : Exemples de configuration de recherche

Non.	DN de base LDAP	Portée de la recherche	Attribut de nommage	Résultat
1	group= Ingénierie,ou=Personnes,dc=ExempleSociété, dc=com	Un niveau	cn=Employé1	Recherche plus rapide
2	dc=ExempleSociété,dc=com	Sous-arborescence	cn=Employé1	Recherche plus longue

Lier à un serveur LDAP

L'ASA utilise le nom de domaine (DN) de connexion et le mot de passe de connexion pour établir la confiance (liaison) avec un serveur LDAP. Lors d'une opération en lecture seule Microsoft Active Directory (comme l'authentification, l'autorisation ou la recherche de groupe), l'ASA peut se lier à l'aide d'un DN de connexion avec moins de privilèges. Par exemple, le DN de connexion peut être un utilisateur dont la désignation AD « Membre de » fait partie des utilisateurs de domaine. Pour les opérations de gestion des mots de passe VPN, le nom de domaine de connexion a besoin de privilèges élevés et doit faire partie du groupe AD des opérateurs de compte.

Remarque Lors de la configuration de l'authentification LDAP sur les périphériques Firepower 1000/2100, évitez d'utiliser une barre oblique inverse (« \ ») dans le mot de passe de liaison. La présence d'une barre oblique inverse dans le mot de passe entraîne l'échec du processus de liaison LDAP, ce qui entraîne l'échec de l'authentification extérieure.

Voici un exemple de DN de connexion :

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

L'ASA prend en charge les méthodes d'authentification suivantes :

- Authentification LDAP simple avec un mot de passe non chiffré sur le port 389
- LDAP sécurisé (LDAP-S) sur le port 636
- Couche d'authentification et de sécurité simple (SASL) MD5
- SASL Kerberos

L'ASA ne prend pas en charge l'authentification anonyme.

Remarque En tant que client LDAP, l'ASA ne prend pas en charge la transmission de liaisons ou de demandes anonymes.

Cartes d'attribut LDAP

L'ASA peut utiliser un répertoire LDAP pour authentifier les utilisateurs pour :

- Les utilisateurs VPN d'accès à distance
- Les sessions d'accès au réseau du pare-feu/de mandataire direct
- La définition des autorisations de politique (également appelées attributs d'autorisation), telles que les ACL, les listes de signets, les paramètres DNS ou WINS et les minuteries de session.
- La définition des attributs clés dans une stratégie de groupe locale

L'ASA utilise des cartes d'attributs LDAP pour traduire les attributs des utilisateurs LDAP natifs en attributs ASA. Vous pouvez lier ces cartes d'attributs aux serveurs LDAP ou les supprimer. Vous pouvez également afficher ou effacer les cartes d'attributs.

La carte d'attributs LDAP ne prend pas en charge les attributs à valeurs multiples. Par exemple, si un utilisateur est membre de plusieurs groupes AD et que la carte d'attributs LDAP correspond à plusieurs groupes, la valeur choisie est basée sur l'ordre alphabétique des entrées correspondantes.

Pour utiliser correctement les fonctionnalités de mappage d'attributs, vous devez comprendre les noms et les valeurs des attributs LDAP, ainsi que les noms et les valeurs des attributs définis par l'utilisateur.

Les noms des attributs LDAP fréquemment mappés et le type d'attributs définis par l'utilisateur auxquels ils sont généralement mappés sont les suivants :

- IETF-Radius-Class (Group_Policy dans ASA version 8.2 et ultérieure) : définit la stratégie de groupe en fonction de la valeur d'attribut du service répertoire ou du groupe d'utilisateurs (par exemple, Microsoft Active Directory memberOf). L'attribut de stratégie de groupe a remplacé l'attribut IETF-Radius-Class par ASDM version 6.2/ASA version 8.2 ou ultérieure.
- IETF-Radius-Filter-Id : applique une liste de contrôle d'accès ou une ACL aux clients VPN, IPsec et SSL.
- IETF-Radius-Framed-IP-Address : attribue une adresse IP statique à un client d'accès à distance VPN, IPsec et SSL.
- Banner1 : affiche une bannière de texte lorsque l'utilisateur d'accès à distance VPN se connecte.
- Tunneling-Protocols : autorise ou refuse la session d'accès à distance VPN en fonction du type d'accès.

Remarque Une seule carte d'attributs LDAP peut contenir un ou plusieurs attributs. Vous ne pouvez mapper qu'un seul attribut LDAP à partir d'un serveur LDAP donné.

Lignes directrices relatives aux serveurs LDAP pour AAA

Cette section inclut des lignes directrices et des limites que vous devez vérifier avant de configurer les serveurs LDAP pour l'AAA.

IPv6

Le serveur AAA peut utiliser une adresse IPv4 ou IPv6.

Directives supplémentaires

- Le DN configuré sur l'ASA pour accéder à un serveur de répertoire Sun doit pouvoir accéder à la politique de mot de passe par défaut sur ce serveur. Nous vous conseillons d'utiliser l'administrateur de répertoire ou un utilisateur disposant des privilèges d'administrateur de répertoire, comme DN. Vous pouvez également placer une ACL sur la politique de mot de passe par défaut.
- Vous devez configurer LDAP sur SSL pour activer la gestion des mots de passe avec les serveurs Microsoft Active Directory et Sun.
- L'ASA ne prend pas en charge la gestion des mots de passe avec Novell, OpenLDAP et les autres serveurs de répertoire LDAPv3.
- À partir de la version 7.1(x), l'ASA effectue l'authentification et l'autorisation à l'aide du schéma LDAP natif, et le schéma Cisco n'est plus nécessaire.
- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 4 groupes de serveurs par contexte en mode multiple.
- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple.
- Lorsqu'un utilisateur se connecte, les serveurs LDAP sont accessibles un par un en commençant par le premier serveur que vous spécifiez dans la configuration, jusqu'à ce qu'un serveur réponde. Si tous les serveurs du groupe sont indisponibles, l'ASA essaie la base de données locale si vous l'avez configurée

comme méthode de secours (authentification et autorisation de gestion uniquement). Si vous n'avez pas de méthode de secours, l'ASA continue d'essayer les serveurs LDAP.

Configurer les serveurs LDAP pour AAA

Cette section décrit comment configurer les serveurs LDAP pour AAA.

Procédure

Étape 1 Configurez les cartes d'attributs LDAP. Consultez Configurer les cartes d'attribut LDAP, à la page 1114.

Étape 2 Ajoutez un groupe de serveurs LDAP. Consultez Configurer les groupes de serveurs LDAP, à la page 1115.

Étape 3 Ajoutez un serveur au groupe, puis configurez les paramètres du serveur. Consultez Ajouter un serveur LDAP à un groupe de serveurs , à la page 1116.

Configurer les cartes d'attribut LDAP

Pour configurer les cartes d'attributs LDAP, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **AAA Local Users (Utilisateurs locaux AAA)** > **LDAP Attribute Map (Carte d'attributs LDAP)** (pour les utilisateurs locaux) ou **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **LDAP Attribute Map (Carte d'attributs LDAP)** (pour tous les autres utilisateurs), puis cliquez sur **Add**.

La boîte de dialogue **Add LDAP Attribute Map** (Ajouter une carte d'attributs LDAP) s'affiche et l'onglet **Mapping of Attribute Name** (Mappage du nom d'attribut) est actif.

Étape 2 Créez un nom pour cette carte d'attributs.

Étape 3 Ajoutez le nom de l'un des attributs LDAP à mapper.

Étape 4 Choisissez un attribut Cisco.

Étape 5 Cliquez sur **Add** (ajouter).

Étape 6 Pour mapper d'autres attributs, répétez les étapes 1 à 5.

Étape 7 Cliquez sur l'onglet **Mappage of Attribute Value** (Mappage de la valeur d'attribut) pour mapper la valeur de l'un des attributs LDAP à une nouvelle valeur dans l'attribut Cisco mappé.

Étape 8 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Mapping of Attribute Value** (Ajouter le mappage de la valeur d'attribut).

Étape 9 Saisissez la valeur de cet attribut LDAP que vous souhaitez renvoyer par le serveur LDAP.

Étape 10 Saisissez la valeur que vous souhaitez utiliser dans l'attribut Cisco lorsque cet attribut LDAP contient la valeur d'attribut LDAP précédente.

Étape 11 Cliquez sur **Add** (ajouter).

Étape 12 Pour mapper d'autres valeurs d'attribut, répétez les étapes 8 à 11.

Étape 13 Cliquez sur **OK** deux fois pour fermer chaque boîte de dialogue.

Étape 14 Cliquez sur **Apply** (Appliquer) pour enregistrer les paramètres dans la configuration d'exécution.

Configurer les groupes de serveurs LDAP

Pour créer et configurer un groupe de serveurs LDAP, puis ajouter un serveur LDAP à ce groupe, procédez comme suit :

Avant de commencer

Vous devez ajouter une mise en correspondance d'attributs avant de pouvoir ajouter un serveur LDAP à un groupe de serveurs LDAP.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)** ou **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **AAA/Local Users (AAA/Utilisateurs locaux)** > **AAA Server Groups (Groupes de serveurs AAA)** pour les utilisateurs VPN.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) apparaît.

Étape 3 Saisissez un nom pour le groupe de serveurs AAA.

Étape 4 Dans la liste déroulante **Protocol** (Protocole), choisissez le type de serveur LDAP.

Étape 5 Cliquez sur le bouton radio du mode de réactivation que vous souhaitez utiliser (**Depletion** (Épuisement) ou **Timed** (Temporisé)).

En mode Depletion (Épuisement), les serveurs défaillants ne sont réactivés qu'une fois que tous les serveurs du groupe sont inactifs.

En mode Timed (Temporisé), les serveurs défaillants sont réactivés après 30 secondes de temps d'arrêt.

a) Si vous avez choisi le mode de réactivation Depletion (Épuisement), saisissez un intervalle de temps dans le champ **Dead Time** (Temps mort).

Le temps mort est la durée, en minutes, qui s'écoule entre la désactivation du dernier serveur d'un groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort.

Étape 6 Ajoutez le nombre maximum de transactions AAA échouées avec le serveur à autoriser.

Cette option définit le nombre de tentatives de connexion échouées autorisées avant de déclarer inactif un serveur qui ne répond pas.

Étape 7 Cliquez sur **OK**.

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) se ferme et le nouveau groupe de serveurs est ajouté au groupe de serveurs AAA.

Étape 8 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Ajouter un serveur LDAP à un groupe de serveurs

Pour ajouter un serveur LDAP à un groupe de serveurs, procédez comme suit :

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

- **Configuration Remote Access VPN (VPN d'accès à distance) AAA/Local Users (AAA/Utilisateurs locaux) AAA Server Groups (Groupes de serveurs AAA)** pour les utilisateurs VPN.
- **Configuration** >**Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**

Étape 2 Sélectionnez le groupe de serveurs auquel vous souhaitez ajouter un serveur, puis cliquez sur **Add**.

La boîte de dialogue **Add AAA Server** (Ajouter un serveur AAA) s'affiche pour le groupe de serveurs sélectionné.

Étape 3 Choisissez le nom de l'interface qui se connecte au serveur LDAP.

Étape 4 Ajoutez le nom du serveur ou l'adresse IP du serveur LDAP.

Étape 5 Ajoutez une valeur de délai d'expiration ou conservez la valeur par défaut. Le délai d'expiration est la durée, en secondes, pendant laquelle l'ASA attend une réponse du serveur principal avant d'envoyer la demande au serveur de sauvegarde.

Étape 6 Dans la zone **LDAP Parameters for authentication/authorization** (Paramètres LDAP pour l'authentification/l'autorisation), configurez les paramètres suivants :

- **Enable LDAP over SSL** (Activer LDAP sur SSL) (également appelé LDAP sécurisé ou LDAP-S) : cochez cette case pour utiliser SSL pour sécuriser les communications entre l'ASA et le serveur LDAP.

Remarque Si vous ne configurez pas le protocole SASL, nous vous conseillons fortement de sécuriser les communications LDAP avec SSL.

- **Reference Identity Name** (Nom d'identité de référence) : saisissez le nom d'identité de référence pour valider l'identité du serveur LDAP.
- **Server Port** (Port du serveur) : saisissez le numéro de port TCP 389, le port utilisé par l'ASA pour accéder au serveur LDAP pour l'authentification simple (non sécurisée), ou le port TCP 636 pour l'authentification sécurisée (LDAP-S). Tous les serveurs LDAP prennent en charge l'authentification et l'autorisation. Seuls les serveurs Microsoft AD et Sun LDAP fournissent en outre une fonctionnalité de gestion des mots de passe d'accès à distance VPN, qui nécessite LDAP-S.

- **Server Type** (Type de serveur) : spécifiez le type de serveur LDAP dans la liste déroulante. Les options disponibles sont les suivantes :
  - **Détection automatique/Utilisation du type générique**
  - **Microsoft**
  - **Novell**
  - **OpenLDAP**
  - **Sun, qui fait désormais partie d'Oracle Directory Server Enterprise Edition**
- **Base DN** (DN de base) : saisissez le nom distinctif (DN) de base ou l'emplacement dans la hiérarchie LDAP où le serveur doit commencer la recherche lorsqu'il reçoit une demande LDAP (par exemple, OU=people, dc=cisco, dc=com).
- **Scope** (Portée) : spécifiez l'étendue de la recherche que le serveur doit effectuer dans la hiérarchie LDAP lorsqu'il reçoit une demande d'autorisation à partir de la liste déroulante. Les options suivantes sont disponibles :
  - **One Level** (Un niveau) : recherche dans un seul niveau sous le DN de base. Cette option est plus rapide.
  - **All Levels** (Tous les niveaux) : recherche dans tous les niveaux sous le DN de base (c'est-à-dire dans la hiérarchie complète des sous-arborescences). Cette option prend plus de temps.
- **Naming Attribute(s)** (Attribut(s) de dénomination) : saisissez le ou les attributs de nom distinctif relatifs qui identifient de manière unique une entrée sur le serveur LDAP. Les attributs de dénomination courants sont Common Name (CN), sAMAccountName, userPrincipalName et User ID (uid).
- **Login DN and Login Password** (DN de connexion et mot de passe de connexion) : l'ASA utilise le DN de connexion et le mot de passe de connexion pour établir la confiance (liaison) avec un serveur LDAP. Précisez le mot de passe de connexion, qui est le mot de passe du compte d'utilisateur DN de connexion.
- **LDAP Attribute Map** (Carte d'attributs LDAP) : sélectionnez l'une des cartes d'attributs que vous avez créées pour ce serveur LDAP à utiliser. Ces cartes d'attributs mappent les noms d'attributs LDAP aux noms et aux valeurs d'attributs Cisco.
- **SASL MD5 authentication** (Authentification SASL MD5) : cela permet au mécanisme MD5 du SASL d'authentifier les communications entre l'ASA et le serveur LDAP.
- **SASL Kerberos authentication** (Authentification SASL Kerberos) : permet au mécanisme Kerberos du SASL de sécuriser les communications d'authentification entre l'ASA et le serveur LDAP. Vous devez avoir défini un serveur Kerberos pour activer cette option.
- **LDAP Parameters for Group Search** (Paramètres LDAP pour la recherche de groupes) : les champs de cette zone configurent la façon dont l'ASA demande les groupes AD.
  - **Group Base DN** (DN de base du groupe) : spécifie l'emplacement dans la hiérarchie LDAP pour commencer la recherche des groupes AD (c'est-à-dire la liste des énumérations memberOf). Si ce champ n'est pas configuré, l'ASA utilise le DN de base pour la récupération du groupe AD. ASDM utilise la liste des groupes AD récupérés pour définir les critères de sélection AAA pour les politiques d'accès dynamique. Pour en savoir plus, consultez la page de la commande **show ad-groups**.
  - **Group Search Timeout** (Délai d'expiration de la recherche de groupe) : spécifiez le temps d'attente maximum d'une réponse d'un serveur AD qui a été interrogé pour les groupes disponibles.

- **LDAP SSL Client Certificate/Client Identity Certificate Trustpoint** (Point de confiance du certificat client SSL LDAP/certificat d'identité du client) : si vous activez LDAP sur SSL, vous pouvez sélectionner le point de confiance du certificat que le client ASA doit présenter au serveur LDAP pour authentification. Un point de confiance est requis si vous configurez le serveur LDAP pour authentifier les certificats clients. Si vous ne configurez pas de certificat, l'ASA n'en présente pas lorsque le serveur LDAP le demande. Si un serveur LDAP est configuré pour nécessiter un certificat homologue, la session LDAP sécurisée ne se terminera pas, et les demandes d'authentification ou d'autorisation échoueront.

Étape 7 Cliquez sur **OK**.

La boîte de dialogue **Add AAA Server** (Ajouter un serveur AAA) se ferme et le serveur AAA est ajouté au groupe de serveurs AAA.

Étape 8 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Tester l'authentification et l'autorisation du serveur LDAP

Pour déterminer si l'ASA peut communiquer avec un serveur LDAP et authentifier ou autoriser un utilisateur, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Sélectionnez le groupe de serveurs dans lequel se trouve le serveur.

Étape 3 Sélectionnez le serveur que vous souhaitez tester.

Étape 4 Cliquez sur **Test**.

La boîte de dialogue **Test AAA Server** (Tester un serveur AAA) s'affiche pour le groupe de serveurs sélectionné.

Étape 5 Cliquez sur le type de test que vous souhaitez effectuer : **Authentication** (Authentification) ou **Authorization** (Autorisation).

Étape 6 Saisissez un nom d'utilisateur.

Étape 7 Si vous testez l'authentification, saisissez le mot de passe correspondant au nom d'utilisateur.

Étape 8 Cliquez sur **OK**.

L'ASA envoie un message de test d'authentification ou d'autorisation au serveur. Si le test échoue, un message d'erreur s'affiche.

Supervision des serveurs LDAP pour AAA

Consultez les commandes suivantes pour superviser les serveurs LDAP pour AAA :

- **Monitoring (Supervision) > Properties (Propriétés) > AAA Servers (Serveurs AAA)**

  Ce volet affiche les statistiques du serveur AAA configuré.

- **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

Historique des serveurs LDAP pour AAA

Tableau 56 : Historique des serveurs AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs LDAP pour AAA	7.0(1)	Les serveurs LDAP décrivent la prise en charge d'AAA et la configuration des serveurs LDAP. Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Server Groups Configuration (Configuration des groupes de serveurs AAA) > Remote Access VPN (VPN d'accès à distance) > AAA Local Users (Utilisateurs locaux AAA) > LDAP Attribute Map (Carte d'attributs LDAP).
Serveurs LDAP avec adresses IPv6 pour AAA	9.7(1)	Vous pouvez maintenant utiliser une adresse IPv4 ou IPv6 pour le serveur AAA.
Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe.	9.13(1)	Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4). En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée. Nous avons modifié les écrans AAA pour accepter ces nouvelles limites.

Nom de la caractéristique	Versions de plateforme	Description
Authentification LDAPS mutuelle.	9.18(1)	Vous pouvez configurer un certificat client que l'ASA doit présenter au serveur LDAP lorsqu'il demande un certificat pour l'authentification. Cette fonctionnalité s'applique lorsque vous utilisez LDAP sur SSL. Si un serveur LDAP est configuré pour nécessiter un certificat homologue, la session LDAP sécurisée ne se terminera pas, et les demandes d'authentification ou d'autorisation échoueront. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > > **AAA Server Groups (Groupes de serveurs AAA)**, Add/Edit LDAP server (Ajouter/modifier un serveur LDAP).



CHAPITRE 42

Serveurs Kerberos pour AAA

Les rubriques suivantes expliquent comment configurer les serveurs Kerberos utilisés dans l'AAA. Vous pouvez utiliser des serveurs Kerberos pour l'authentification des connexions de gestion, l'accès réseau et l'accès utilisateur VPN.

- Lignes directrices relatives aux serveurs Kerberos pour AAA, à la page 1121
- Configurer les serveurs Kerberos pour AAA, à la page 1121
- Superviser les serveurs Kerberos pour AAA, à la page 1125
- Historique des serveurs Kerberos pour AAA, à la page 1125

Lignes directrices relatives aux serveurs Kerberos pour AAA

- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 8 groupes de serveurs par contexte en mode multiple.
- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple. Lorsqu'un utilisateur se connecte, les serveurs sont accessibles un par un en commençant par le premier serveur que vous spécifiez dans la configuration, jusqu'à ce qu'un serveur réponde.

Configurer les serveurs Kerberos pour AAA

Les rubriques suivantes expliquent comment configurer les groupes de serveurs Kerberos. Vous pouvez ensuite utiliser ces groupes lors de la configuration de l'accès de gestion ou des VPN.

Configurer les groupes de serveurs AAA Kerberos

Si vous souhaitez utiliser un serveur Kerberos pour l'authentification, vous devez d'abord créer au moins un groupe de serveurs Kerberos et ajouter un ou plusieurs serveurs à chaque groupe.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Cliquez sur **Add** (Ajouter) dans le champ **AAA Server Groups** (Groupes de serveurs AAA).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) apparaît.

Étape 3 Saisissez un nom pour le groupe dans le champ **Server Group** (Groupe de serveurs).

Étape 4 Dans la liste déroulante **Protocol** (Protocole), choisissez le type de serveur **Kerberos** :

Étape 5 Cliquez sur **Depletion** (Épuisement) ou **Timed** (Temporisé) dans le champ **Reactivation Mode** (Mode de réactivation).

En mode Depletion (Épuisement), les serveurs défaillants ne sont réactivés qu'une fois que tous les serveurs du groupe sont inactifs. En mode d'épuisement, lorsqu'un serveur est désactivé, il reste inactif jusqu'à ce que tous les autres serveurs du groupe soient inactifs. Lorsque et si cela se produit, tous les serveurs du groupe sont réactivés. Cette approche réduit le nombre de retards de connexion en raison de serveurs défaillants.

En mode Timed (Temporisé), les serveurs défaillants sont réactivés après 30 secondes de temps d'arrêt.

Étape 6 Si vous avez choisi le mode de réactivation Depletion (Épuisement), saisissez un intervalle de temps dans le champ **Dead Time** (Temps mort).

Le temps mort est la durée, en minutes, qui s'écoule entre la désactivation du dernier serveur d'un groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort.

Étape 7 Précisez le nombre maximum de transactions AAA échouées avec un serveur AAA du groupe avant d'essayer le serveur suivant.

Cette option définit le nombre de transactions AAA ayant échoué avant de déclarer inactif un serveur qui ne répond pas.

Étape 8 (Facultatif) Sélectionnez **Validate KDC** (Valider le KDC) pour activer la validation du centre de distribution des clés de Kerberos (KDC).

Pour réaliser l'authentification, vous devez également importer un fichier keytab que vous avez exporté du centre de distribution des clés Kerberos (KDC). En validant le KDC, vous pouvez empêcher une attaque où l'agresseur usurpe le KDC de sorte que les informations d'authentification de l'utilisateur soient authentifiées sur le serveur Kerberos de l'agresseur.

Pour savoir comment charger le fichier keytab, consultez Configurer la validation du centre de distribution des clés Kerberos, à la page 1123.

Étape 9 Cliquez sur **OK**.

Ajouter des serveurs Kerberos à un groupe de serveurs Kerberos

Avant de pouvoir utiliser un groupe de serveurs Kerberos, vous devez ajouter au moins un serveur Kerberos au groupe.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Sélectionnez le groupe de serveurs auquel vous souhaitez ajouter un serveur.

Étape 3 Cliquez sur **Add** (Ajouter) dans la zone **Servers in the Selected Group** (Serveurs du groupe sélectionné).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) s'affiche pour le groupe de serveurs.

Étape 4 Choisissez l'**Interface Name** (Nom de l'interface) dans lequel se trouve le serveur d'authentification.

Étape 5 Saisissez le nom ou l'adresse IP du serveur que vous ajoutez au groupe.

Étape 6 Spécifiez la valeur du délai d'expiration pour les tentatives de connexion au serveur.

Spécifiez l'intervalle du délai d'expiration (1 à 300 secondes) du serveur; la valeur par défaut est de 10 secondes. Pour chaque transaction AAA, l'ASA relance les tentatives de connexion (en fonction de l'intervalle de nouvelle tentative) jusqu'à ce que le délai d'expiration soit atteint. Si le nombre de transactions consécutives ayant échoué atteint la limite maximum-failed-attempts spécifiée dans le groupe de serveurs AAA, le serveur AAA est désactivé et l'ASA commence à envoyer des demandes à un autre serveur AAA s'il est configuré.

Étape 7 Sélectionnez l'intervalle entre les tentatives, qui correspond au temps d'attente du système avant de réessayer une demande de connexion. Vous pouvez sélectionner de 1 à 10 secondes. La valeur par défaut est de 10 secondes.

Étape 8 Spécifiez le Server Port (Port du serveur). Le port du serveur est le numéro de port 88 ou le numéro de port TCP utilisé par l'ASA pour communiquer avec le serveur Kerberos.

Étape 9 Configurez le domaine Kerberos.

Les noms de domaine Kerberos utilisent uniquement des chiffres et des lettres majuscules et peuvent comporter jusqu'à 64 caractères. Le nom doit correspondre à la sortie de la commande Microsoft Windows **set USERDNSDOMAIN** lorsqu'elle est exécutée sur le serveur Active Directory pour le domaine Kerberos. Dans l'exemple suivant, EXEMPLE.COM est le nom de domaine Kerberos :

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

Bien que l'ASA accepte les lettres minuscules dans le nom, il ne convertit pas les lettres minuscules en majuscules. Assurez-vous d'utiliser uniquement des lettres majuscules.

Étape 10 Cliquez sur **OK**.

Exemple

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

Configurer la validation du centre de distribution des clés Kerberos

Vous pouvez configurer un groupe de serveurs AAA Kerberos pour authentifier les serveurs du groupe. Pour réaliser l'authentification, vous devez importer un fichier keytab que vous avez exporté du centre de distribution

des clés Kerberos (KDC). En validant le KDC, vous pouvez empêcher une attaque où l'agresseur usurpe le KDC de sorte que les informations d'authentification de l'utilisateur soient authentifiées sur le serveur Kerberos de l'agresseur.

Lorsque vous activez la validation KDC, après avoir obtenu le billet d'octroi de billets (TGT) et validé l'utilisateur, le système demande également un billet de service au nom de l'utilisateur pour host/ASA_hostname. Le système valide ensuite le billet de service renvoyé par rapport à la clé secrète du KDC, qui est stockée dans un fichier keytab que vous avez généré à partir du KDC, puis téléchargé sur l'ASA. En cas d'échec de l'authentification KDC, le serveur est considéré comme non fiable et l'utilisateur n'est pas authentifié.

La procédure suivante explique comment réaliser l'authentification KDC.

Avant de commencer

Vous ne pouvez pas utiliser la validation KDC conjointement avec la délégation Kerberos contrainte (KCD). La commande option de validation KDC sera ignorée si le groupe de serveurs est utilisé pour le KCD.

Procédure

Étape 1 (Sur le KDC.) Créez un compte d'utilisateur dans Microsoft Active Directory pour l'ASA (accédez à **Start (Démarrage)** > **Programs (Programmes)** > **Administrative Tools (Outils administratifs)** > **Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)**). Par exemple, si le nom de domaine complet (FQDN) de l'ASA est asahost.example.com, créez un utilisateur nommé asahost.

Étape 2 (Sur le KDC.) Créez un nom principal de service d'hôte (SPN) pour l'ASA à l'aide du FQDN et du compte d'utilisateur :

```
C:> setspn -A HOST/asahost.example.com asahost
```

Étape 3 (Sur le KDC.) Créez un fichier keytab pour l'ASA (des sauts de ligne ont été ajoutés pour plus de clarté) :

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

Étape 4 (Sur l'ASA.) Choisissez **Tools (Outils)** > **File Management (Gestion des fichiers)**, puis dans le menu **File Transfer (Transfert de fichiers)**, sélectionnez l'option appropriée pour charger le fichier keytab dans la mémoire flash, selon s'il se trouve sur votre ordinateur ou sur un serveur distant.

Étape 5 (Sur l'ASA.) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Kerberos**, puis cliquez sur **Browse Flash** (Parcourir la mémoire flash) et sélectionnez le fichier keytab chargé.

Étape 6 (Sur l'ASA.) Ajoutez l'option **Validate KDC** (Valider le KDC) à la configuration du groupe de serveurs AAA Kerberos. Le fichier keytab est utilisé uniquement par les groupes de serveurs configurés avec cette option.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

b) Sélectionnez le groupe de serveurs Kerberos et cliquez sur **Edit** (Modifier). Vous pouvez également créer un nouveau groupe à ce stade.

c) Sélectionnez l'option **Validate KDC** (Valider le KDC).
d) Cliquez sur **OK**.

Superviser les serveurs Kerberos pour AAA

Vous pouvez utiliser les commandes suivantes pour superviser et effacer les renseignements relatifs à Kerberos. Saisissez les commandes dans la fenêtre **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

- **Monitoring (Supervision)** > **Properties (Propriétés)** > **AAA Servers (Serveurs AAA)**

  Cette fenêtre affiche les statistiques du serveur AAA.

- **show aaa-server**

  Affiche les statistiques du serveur AAA. Utilisez la commande **clear aaa-server statistics** pour effacer les statistiques du serveur.

- **show running-config aaa-server**

  Affiche les serveurs AAA configurés pour le système. Utilisez la commande **clear configure aaa-server** pour supprimer la configuration du serveur AAA.

- **show aaa kerberos** [**username** *utilisateur*]

  Affiche tous les billets Kerberos ou les billets pour un nom d'utilisateur donné.

- **clear aaa kerberos tickets** [**username** *utilisateur*]

  Efface tous les billets Kerberos ou les billets pour un nom d'utilisateur donné.

- **show aaa kerberos keytab**

  Affiche des renseignements sur le fichier keytab Kerberos.

- **clear aaa kerberos keytab**

  Efface le fichier keytab Kerberos.

Historique des serveurs Kerberos pour AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs Kerberos	7.0(1)	Prise en charge des serveurs Kerberos pour AAA. Nous avons introduit les écrans suivants : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**
Adresses IPv6 pour AAA	9.7(1)	Vous pouvez maintenant utiliser une adresse IPv4 ou IPv6 pour le serveur AAA.

Nom de la caractéristique	Versions de plateforme	Description
Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe.	9.13(1)	Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4). En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée. Nous avons modifié les écrans AAA pour accepter ces nouvelles limites.
Authentification du centre de distribution des clés Kerberos (KDC).	9.8(4) et versions provisoires ultérieures jusqu'à 9.14(1)	Vous pouvez importer un fichier keytab à partir d'un centre de distribution de clés (KDC) Kerberos, et le système peut authentifier que le serveur Kerberos n'est pas falsifié avant de l'utiliser pour authentifier les utilisateurs. Pour réaliser l'authentification par KDC, vous devez configurer un nom de principal de service (SPN) **hôte**/*ASA_hostname* sur le KDC Kerberos, puis exporter un fichier keytab pour ce SPN. Vous devez ensuite charger le fichier keytab sur l'ASA et configurer le groupe de serveurs AAA Kerberos pour valider le KDC. Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Kerberos**, **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)** Add/Edit dialog box for Kerberos server groups (Boîte de dialogue Ajouter/Modifier pour les groupes de serveurs Kerberos).



CHAPITRE 43

Configurer les serveurs RSA SecurID pour AAA

Les rubriques suivantes expliquent comment configurer les serveurs RSA SecurID utilisés dans l'AAA. Les serveurs RSA SecureID sont également connus sous le nom de serveurs SDI, car SDI est le protocole utilisé pour communiquer avec eux. Vous pouvez utiliser des serveurs RSA SecurID pour l'authentification des connexions de gestion, l'accès réseau et l'accès utilisateur VPN.

- À propos des serveurs RSA SecurID, à la page 1127
- Lignes directrices relatives aux serveurs RSA SecurID pour AAA, à la page 1127
- Configurer les serveurs RSA SecurID pour AAA, à la page 1128
- Superviser les serveurs RSA SecurID pour AAA, à la page 1130
- Historique des serveurs RSA SecurID pour AAA, à la page 1131

À propos des serveurs RSA SecurID

Vous pouvez utiliser des serveurs RSA SecurID directement pour l'authentification, ou indirectement, comme deuxième facteur d'authentification. Dans ce dernier cas, vous devez configurer la relation avec le serveur SecurID entre le serveur SecurID et votre serveur RADIUS, et configurer l'ASA pour utiliser le serveur RADIUS.

Mais, si vous souhaitez vous authentifier directement auprès du serveur SecurID, vous devez créer un groupe de serveurs AAA pour le protocole SDI, qui est le protocole utilisé pour communiquer avec ces serveurs.

Lorsque vous utilisez SDI, vous n'avez qu'à préciser le serveur SecurID principal lorsque vous créez le groupe de serveurs AAA. L'ASA récupérera le fichier sdiconf.rec, qui répertorie toutes les répliques de serveur SecurID, lors de sa première connexion au serveur. L'ASA peut ensuite utiliser ces répliques pour l'authentification si le serveur principal ne répond pas.

En outre, vous devez enregistrer l'ASA en tant qu'agent d'authentification dans le gestionnaire d'authentification RSA. Les tentatives d'authentification échoueront jusqu'à ce que vous enregistriez l'ASA.

Lignes directrices relatives aux serveurs RSA SecurID pour AAA

- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 8 groupes de serveurs par contexte en mode multiple.

- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple. Lorsqu'un utilisateur se connecte, les serveurs sont accessibles un par un en commençant par le premier serveur que vous spécifiez dans la configuration, jusqu'à ce qu'un serveur réponde.

Configurer les serveurs RSA SecurID pour AAA

Les rubriques suivantes expliquent comment configurer les groupes de serveurs RSA SecurID. Vous pouvez ensuite utiliser ces groupes lors de la configuration de l'accès de gestion ou des VPN.

Configurer les groupes de serveurs RSA SecurID pour AAA

Si vous souhaitez utiliser la communication directe avec un serveur RSA SecurID pour l'authentification, vous devez d'abord créer au moins un groupe de serveurs SDI et ajouter un ou plusieurs serveurs à chaque groupe. Si vous utilisez le serveur SecurID dans une relation mandataire avec un serveur RADIUS, il n'est pas nécessaire de configurer un groupe de serveurs AAA SDI sur l'ASA.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Cliquez sur **Add** (Ajouter) dans le champ **AAA Server Groups** (Groupes de serveurs AAA).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) apparaît.

Étape 3 Saisissez un nom pour le groupe dans le champ **Server Group** (Groupe de serveurs).

Étape 4 Dans la liste déroulante **Protocol** (Protocole), choisissez le type de serveur **SDI** :

Étape 5 Cliquez sur **Depletion** (Épuisement) ou **Timed** (Temporisé) dans le champ **Reactivation Mode** (Mode de réactivation).

En mode Depletion (Épuisement), les serveurs défaillants ne sont réactivés qu'une fois que tous les serveurs du groupe sont inactifs. En mode d'épuisement, lorsqu'un serveur est désactivé, il reste inactif jusqu'à ce que tous les autres serveurs du groupe soient inactifs. Lorsque et si cela se produit, tous les serveurs du groupe sont réactivés. Cette approche réduit le nombre de retards de connexion en raison de serveurs défaillants.

En mode Timed (Temporisé), les serveurs défaillants sont réactivés après 30 secondes de temps d'arrêt.

Étape 6 Si vous avez choisi le mode de réactivation Depletion (Épuisement), saisissez un intervalle de temps dans le champ **Dead Time** (Temps mort).

Le temps mort est la durée, en minutes, qui s'écoule entre la désactivation du dernier serveur d'un groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort.

Étape 7 Précisez le nombre maximum de transactions AAA échouées avec un serveur AAA du groupe avant d'essayer le serveur suivant.

Cette option définit le nombre de transactions AAA ayant échoué avant de déclarer inactif un serveur qui ne répond pas.

Étape 8 Cliquez sur **OK**.

Ajouter des serveurs RSA SecurID à un groupe de serveurs SDI

Avant de pouvoir utiliser un groupe de serveurs SDI, vous devez ajouter au moins un serveur RSA SecurID au groupe.

Les serveurs d'un groupe de serveurs SDI utilisent le protocole d'authentification et de gestion de serveur (ACE) pour communiquer avec l'ASA.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Sélectionnez le groupe de serveurs auquel vous souhaitez ajouter un serveur.

Étape 3 Cliquez sur **Add** (Ajouter) dans la zone **Servers in the Selected Group** (Serveurs du groupe sélectionné).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) s'affiche pour le groupe de serveurs.

Étape 4 Choisissez l'**Interface Name** (Nom de l'interface) dans lequel se trouve le serveur d'authentification.

Étape 5 Saisissez le nom ou l'adresse IP du serveur que vous ajoutez au groupe.

Étape 6 Spécifiez la valeur du délai d'expiration pour les tentatives de connexion au serveur.

Spécifiez l'intervalle du délai d'expiration (1 à 300 secondes) du serveur; la valeur par défaut est de 10 secondes. Pour chaque transaction AAA, l'ASA relance les tentatives de connexion (en fonction de l'intervalle de nouvelle tentative) jusqu'à ce que le délai d'expiration soit atteint. Si le nombre de transactions consécutives ayant échoué atteint la limite maximum-failed-attempts spécifiée dans le groupe de serveurs AAA, le serveur AAA est désactivé et l'ASA commence à envoyer des demandes à un autre serveur AAA s'il est configuré.

Étape 7 Sélectionnez l'intervalle entre les tentatives, qui correspond au temps d'attente du système avant de réessayer une demande de connexion. Vous pouvez sélectionner de 1 à 10 secondes. La valeur par défaut est de 10 secondes.

Étape 8 Spécifiez le Server Port (Port du serveur). Le port du serveur est le numéro de port 5500 par défaut ou le numéro de port TCP utilisé par l'ASA pour communiquer avec le serveur RSA SecurID.

Étape 9 Cliquez sur **OK**.

Importer le fichier secret de nœud SDI

Vous pouvez importer manuellement le fichier secret du nœud généré par le serveur RSA Authentication Manager (SecurID).

Procédure

Étape 1 Exportez le fichier secret du nœud à partir du serveur RSA Authentication Manager. Pour en savoir plus, consultez la documentation de RSA Authentication Manager.

Étape 2 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA SDI**.

Étape 3 Cliquez sur **Upload** (Charger), sélectionnez le fichier secret du nœud décompressé qui a été exporté depuis le RSA Authentication Manager, puis chargez-le sur le système.

Étape 4 Sous **Import Node Secret for SDI** (Importer le secret du nœud pour SDI), saisissez les renseignements suivants :

- **Server IP** (Adresse IP du serveur) : l'adresse IP ou le nom d'hôte complet du serveur RSA Authentication Manager auquel appartient le secret du nœud.
- **Password** (Mot de passe) : le mot de passe utilisé pour protéger le fichier lorsque vous l'avez exporté.
- **File Name** (Nom de fichier) : cliquez sur **Browse** (Parcourir) et sélectionnez le fichier secret du nœud décompressé que vous avez chargé.

Superviser les serveurs RSA SecurID pour AAA

Vous pouvez utiliser les commandes suivantes pour superviser et effacer les renseignements relatifs à RSA SecurID. Saisissez les commandes dans la fenêtre **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

- **Monitoring (Supervision)** > **Properties (Propriétés)** > **AAA Servers (Serveurs AAA)**

  Cette fenêtre affiche les statistiques du serveur AAA.

- **show aaa-server**

  Affiche les statistiques du serveur AAA. Utilisez la commande **clear aaa-server statistics** pour effacer les statistiques du serveur.

- **show running-config aaa-server**

  Affiche les serveurs AAA configurés pour le système. Utilisez la commande **clear configure aaa-server** pour supprimer la configuration du serveur AAA.

- **show aaa sdi node-secrets**

  Affiche les serveurs RSA SecurID qui ont un fichier secret de nœud importé. Utilisez la commande **clear aaa sdi node-secret** pour supprimer un fichier secret de nœud.

Historique des serveurs RSA SecurID pour AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs SecurID	7.2(1)	Prise en charge des serveurs SecureID pour AAA pour l'authentification de gestion. SecureID était pris en charge dans les versions précédentes pour l'authentification VPN.
Adresses IPv6 pour AAA	9.7(1)	Vous pouvez maintenant utiliser une adresse IPv4 ou IPv6 pour le serveur AAA.
Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe.	9.13(1)	Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4). En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée. Nous avons modifié les écrans AAA pour accepter ces nouvelles limites.
Importation manuelle du fichier secret du nœud à partir du gestionnaire d'authentification RSA pour les groupes de serveurs AAA SDI.	9.15(1)	Vous pouvez importer le fichier secret du nœud que vous exportez à partir du gestionnaire d'authentification RSA pour l'utiliser avec les groupes de serveurs AAA SDI. Nous avons ajouté l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA SDI**.



PARTIE VII

Administration système

- Accès de gestion, à la page 1135
- Logiciels et configurations, à la page 1185
- Automatisation de la réponse pour les événements système, à la page 1217
- Tests et dépannage, à la page 1225



CHAPITRE 44

Accès de gestion

Ce chapitre décrit comment accéder à l'ASA pour la gestion de systèmes par le biais de Telnet, SSH et HTTPS (à l'aide d'ASDM), authentifier et autoriser les utilisateurs, et créer des bannières de connexion.

- Configurer l'accès de gestion à distance, à la page 1135
- Configurer AAA pour les administrateurs système, à la page 1155
- Accès au moniteur, à la page 1173
- Historique de l'accès de gestion, à la page 1173

Configurer l'accès de gestion à distance

Cette section décrit comment configurer l'accès ASA pour ASDM, Telnet ou SSH, et d'autres paramètres de gestion tels qu'une bannière de connexion.

Configurer l'accès ASA pour HTTPS, Telnet ou SSH

Cette section décrit comment configurer l'accès ASA pour HTTPS (y compris ASDM et CSM), Telnet ou SSH. Consultez les consignes suivantes :

- Pour accéder à l'interface ASA pour l'accès de gestion, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès de gestion conformément aux sections de ce chapitre. Si, toutefois, vous configurez la redirection HTTP pour rediriger automatiquement les connexions HTTP vers HTTPS, vous devez activer un critère d'accès pour autoriser HTTP; sinon, l'interface ne peut pas être à l'écoute du port HTTP.
- L'accès de gestion à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre hôte de gestion est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe. La seule exception à cette règle est une connexion VPN. Consultez Configurer l'accès de gestion sur un tunnel VPN, à la page 1148.
- L'ASA permet :
  - Un maximum de 5 connexions Telnet simultanées par contexte, si disponible, avec un maximum de 100 connexions réparties entre tous les contextes.
  - Un maximum de 5 connexions SSH simultanées par contexte, si disponible, avec un maximum de 100 connexions réparties entre tous les contextes.

- En mode de contexte unique, vous pouvez avoir un maximum de 5 sessions ASDM simultanées. En mode de contexte multiple, vous pouvez avoir un maximum de 5 sessions ASDM simultanées par contexte, avec un maximum de 200 instances ASDM parmi tous les contextes.

  Les sessions ASDM utilisent deux connexions HTTPS: une pour la surveillance qui est toujours présente et une pour apporter des modifications de configuration qui est présente uniquement lorsque vous apportez des modifications. Par exemple, la limite système en mode de contexte multiple de 200 sessions ASDM représente une limite de 400 sessions HTTPS.

- Un maximum de 6 sessions HTTPS non ASDM simultanées en mode de contexte unique ou par contexte, si disponible, avec un maximum de 100 sessions HTTPS parmi tous les contextes.

Configurer l'accès HTTPS pour ASDM, autres clients

Cette section décrit comment configurer l'accès ASA pour HTTPS, y compris ASDM et CSM.

Si vous avez activé SSL (**webvpn** > **enable** *interface*) et l'accès HTTPS sur la même interface, vous pouvez accéder à Secure Client (services client sécurisés) à partir de l'adresse **https://***ip_address* et à ASDM à partir de l'adresse **https://***ip_address***/admin**, tous deux sur le port 443. Si vous activez également l'authentification pour HTTPS (Configurer l'authentification pour l'interface de ligne de commande ASDM et activer la commande Access, à la page 1157), vous devez alors spécifier un port différent pour l'accès à ASDM.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue**Add Device Access Configuration** (Ajouter une configuration d'accès à l'appareil) apparaît.

Étape 2 Choisissez **ASDM/HTTPS**.

Étape 3 Choisissez l'interface de gestion et définissez les adresses IP d'hôte autorisées, puis cliquez sur **OK**.

Spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 1148), spécifiez l'interface BVI nommée.

Étape 4 Pour exiger l'authentification par certificat, dans la zone **Specify the interface requires client certificate to access ASDM** (Spécifier l'interface exige que le certificat client accède à ASDM), cliquez sur **Add** (Ajouter) pour spécifier l'interface et une carte de certificat facultative qui doit être mise en correspondance pour une authentification réussie. Consultez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès au réseau (client))** > **Advanced (Avancé)** > **IPSec** > **Certificate to Connection Map (Certificat pour carte de connexion)** > **Rules (Règles)** pour créer la carte de certificat.

Étape 5 Configurez les **HTTP Settings** (Paramètres HTTP).

- **Enable HTTP server** (Activer le serveur HTTP) : activez le serveur HTTPS.
- **Port Number** (Numéro de port) : définissez le numéro de port. La valeur par défaut est 443.
- **Idle Timeout** (Délai d'inactivité) : définissez le délai d'inactivité pour les connexions ASDM, de 1 à 1 440 minutes. La valeur par défaut est 20 minutes. L'ASA déconnecte une connexion ASDM qui est inactive pendant la période définie.
- **Session Timeout** (Session expirée) : définissez le session expirée pour les sessions ASDM, de 1 à 1 440 minutes. Ce délai est désactivé par défaut. L'ASA déconnecte une session ASDM qui dépasse la période définie.
- **Connection Session Timeout** (Session de connexion expirée) : définissez le délai d'inactivité pour toutes les connexions HTTPS, y compris ASDM, WebVPN et d'autres clients, de 10 à 86 400 secondes. Ce délai est désactivé par défaut. L'ASA déconnecte une connexion qui est inactive pendant la période définie. Si vous définissez **Idle Timeout** (Délai d'inactivité) et **Connection Session Timeout** (Session de connexion expirée), la **Connection Session Timeout** (Session de connexion expirée) prévaut.

Étape 6 Cliquez sur **Apply** (Appliquer).

Étape 7 (Facultatif) Autorisez les clients HTTPS non basés sur le navigateur à accéder aux services HTTPS sur l'ASA. Par défaut, ASDM, CSM et l'API REST sont autorisés.

De nombreux clients spécialistes (par exemple, les bibliothèques python, curl et wget) ne prennent pas en charge l'authentification basée sur le jeton Cross-site Request Forgery (CSRF). Vous devez donc autoriser expressément ces clients à utiliser la méthode d'authentification de base ASA. Pour des raisons de sécurité, vous ne devez autoriser que les clients requis.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **HTTP Non-Browser Client Support (Prise en charge des clients HTTP non basés sur le navigateur)**, puis cliquez sur **Add** (Ajouter).

b) Dans le champ **User-Agent String from the HTTP Header** (Chaîne User-Agent de l'en-tête HTTP), spécifiez la chaîne User-Agent du client dans l'en-tête HTTP de la requête HTTP.

Vous pouvez spécifier la chaîne complète ou une chaîne partielle; les chaînes partielles doivent correspondre au début de la chaîne User-Agent. Nous conseillons d'utiliser des chaînes complètes pour une meilleure sécurité. Notez que la chaîne est sensible à la casse.

Par exemple, **`curl`** correspondra à la chaîne User-Agent suivante :

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

`curl` ne correspondra *pas* à la chaîne User-Agent suivante :

```
abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1
Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

`CURL` ne correspondra *pas* à la chaîne User-Agent suivante :

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

Configurer l'accès SSH

Lignes directrices relatives à SSH

- Pour accéder à l'interface ASA pour l'accès SSH, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès SSH conformément à cette section.
- L'accès SSH à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre hôte SSH est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe. La seule exception à cette règle est une connexion VPN (uniquement prise en charge par la pile ASA SSH). Consultez Configurer l'accès de gestion sur un tunnel VPN, à la page 1148.
- L'ASA permet un maximum de cinq connexions SSH simultanées par contexte/mode unique, avec un maximum de 100 connexions réparties entre tous les contextes. Cependant, comme les commandes de configuration peuvent obtenir des verrouillages sur les ressources en cours de modification, vous devez apporter des modifications à une session SSH à la fois pour vous assurer que toutes les modifications sont appliquées correctement.
- Par défaut, l'ASA utilise la pile CiscoSSH, qui est basée sur OpenSSH. Vous pouvez choisir d'activer à la place la pile ASA SSH propriétaire. CiscoSSH prend en charge :
  - Conformité FIPS
  - Mises à jour régulières, y compris les mises à jour de Cisco et de la communauté de code source libre.

  Notez que la pile CiscoSSH ne prend pas en charge :
  - SSH vers une interface différente sur VPN (accès de gestion)
  - Paire de clés EDDSA
  - Paire de clés RSA en mode FIPS

  Si vous avez besoin de ces fonctionnalités, vous devez utiliser la pile SSH ASA.
- Pour utiliser la commande **copy** de l'ASA afin de copier un fichier vers ou depuis un serveur SCP, vous devez :
  - (Pile CiscoSSH uniquement) Activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP
  - Générer une paire de clés (pour les ASA physiques uniquement)
- Le nom d'utilisateur SSH par défaut n'est plus pris en charge. Vous ne pouvez plus vous connecter à l'ASA à l'aide de SSH avec le nom d'utilisateur **pix** ou **asa** et le mot de passe de connexion. Pour utiliser SSH, vous devez configurer l'authentification AAA en sélectionnant **Configuration** > **Device Management (Gestion de l'appareil)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authentication (Authentification)**; puis définissez un utilisateur local en choisissant **Configuration** > **Device Management (Gestion de l'appareil)** > **Users/AAA (Utilisateurs/AAA)**. Si vous souhaitez utiliser un serveur AAA pour l'authentification au lieu de la base de données locale, nous vous conseillons de configurer également l'authentification locale comme méthode de sauvegarde.
- Seule la version 2 du protocole SSH est prise en charge.

Pour configurer l'accès SSH à l'ASA, activez le serveur SSH et identifiez les adresses IP autorisées. Pour authentifier les utilisateurs, vous pouvez utiliser les méthodes suivantes :

- Nom d'utilisateur et mot de passe utilisant la base de données locale ou un serveur AAA.
- Nom d'utilisateur et clé publique utilisant la base de données locale.

Activer le serveur SSH

Activez le serveur SSH et spécifiez les adresses IP autorisées à se connecter. Vous pouvez également configurer d'autres paramètres du serveur SSH.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.

  Pour définir la pile SSH, terminez la configuration dans l'espace système sur **Configuration** > **Device Management (Gestion des périphériques)** > **SSH Stack (Pile SSH)**.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue**Add Device Access Configuration** (Ajouter une configuration d'accès à l'appareil) apparaît.

Étape 2 Choisissez **SSH**.

Étape 3 Choisissez l'interface de gestion et définissez les adresses IP d'hôte autorisées, puis cliquez sur **OK**.

Spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 1148), spécifiez l'interface BVI nommée.

Étape 4 (Facultatif) Configurez l'option **SSH Settings** (Paramètres SSH).

- **SSH Stack** (Pile SSH) : choisissez **ASA** ou **Cisco**.

Remarque En mode de contexte multiple, consultez **Configuration** > **Device Management (Gestion des périphériques)** > **SSH Stack (Pile SSH)**.

- **SSH Timeout** (Délai d'expiration SSH) : définissez le délai d'expiration entre 1 et 60 minutes. La valeur par défaut est 5 minutes. La durée par défaut est trop courte dans la plupart des cas et doit être augmentée jusqu'à ce que tous les tests et dépannages de pré-production soient terminés.
- **Key Exchange Hostkey** (Clé d'hôte pour l'échange de clés) Par défaut, l'ASA tente d'utiliser les clés dans l'ordre suivant, si elles existent :EdDSA, ECDSA, puis RSA. Si vous choisissez explicitement la clé RSA, vous devez générer une clé de 2 048 bits ou plus. Pour des raisons de compatibilité avec les

mises à niveau, l'ASA utilisera des clés hôtes RSA de plus petite taille uniquement lorsque le paramètre par défaut de la clé hôte est utilisé. La prise en charge des clés RSA sera supprimée dans une version ultérieure. Nous vous suggérons donc d'utiliser les autres types de clés pris en charge.

- **DH Key Exchange** (Échange de clés DH) (Contexte d'administration uniquement) : cliquez sur le bouton radio applicable pour choisir le groupe d'échange de clés Diffie-Hellman (DH). Si aucune méthode d'échange de clés de groupe DH n'est spécifiée, la méthode d'échange de clés Groupe DH 14 SHA256 est utilisée. Pour en savoir plus sur l'utilisation des méthodes d'échange de clés DH, consultez la RFC 4253. Vous ne pouvez définir l'échange de clés que dans le contexte d'administration; cette valeur est utilisée par tous les contextes.

Étape 5 Cliquez sur **Apply** (Appliquer).

Étape 6 (Facultatif) Configurez les algorithmes de chiffrement et d'intégrité SSH :

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffrement SSH)**.

b) Sélectionnez **Encryption** (Chiffrement), puis cliquez sur **Edit** (Modifier).

c) Dans la liste déroulante SSH cipher security level (Niveau de sécurité du chiffrement SSH), choisissez l'un des niveaux suivants.

Les chiffrements sont utilisés dans l'ordre dans lequel ils sont répertoriés. Pour les listes prédéfinies, ils sont répertoriés du plus haut au plus bas niveau de sécurité.

- **All** (Tous) : spécifie l'utilisation de tous les chiffrements : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr chacha20-poly1305@openssh.com aes192-ctr aes256-ctr
- **Custom** (Personnalisé) : spécifie une chaîne de configuration de chiffrement personnalisée que vous saisissez dans le champ **Cipher algorithms/custom string** (Algorithmes de chiffrement/Chaîne personnalisée), séparée par des deux-points.
- **Fips** : spécifie uniquement les chiffrements conformes à la norme FIPS : aes128-cbc aes256-cbc
- **High** spécifie uniquement les chiffrements de force élevée : aes256-cbc chacha20-poly1305@openssh.com aes256-ctr
- **Low** spécifie les chiffrements de force faible, moyenne et élevée : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- **Medium** : spécifie les chiffrements de force moyenne et élevée (par défaut) : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr

d) Sélectionnez **Integrity** (Intégrité), puis cliquez sur **Edit** (Modifier).

e) Dans la liste déroulante SSH cipher security level (Niveau de sécurité du chiffrement SSH), choisissez l'un des niveaux suivants :

- **All** (Tous) : spécifie l'utilisation de tous les chiffrements : hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-md5 hmac-md5-96
- **Custom** (Personnalisé) : spécifie une chaîne de configuration de chiffrement personnalisée que vous saisissez dans le champ **Cipher algorithms/custom string** (Algorithmes de chiffrement/Chaîne personnalisée), séparée par des deux-points.
- **FIPS** : spécifie uniquement les chiffrements conformes à la norme FIPS : hmac-sha1 hmac-sha2-256
- **High** (Élevé) : spécifie uniquement les chiffrements de force élevée (par défaut) : hmac-sha2-256

- **Low** (Faible) : spécifie les chiffrements de force faible, moyenne et élevée : hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96
- **Medium** (Moyen) : spécifie les chiffrements de force moyenne et élevée : hmac-sha1 hmac-sha1-96

Étape 7 Activez le serveur Secure Copy.

a) Selon votre mode de contexte :

- Pour le mode unique, choisissez **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > Secure Copy (SCP) (Copie sécurisée (SCP))**.
- Pour le mode multiple dans le système, choisissez **Configuration > Device Management (Gestion des périphériques) > Device Administration (Administration des périphériques) > Secure Copy (Copie sécurisée)**

b) Cochez la case **Enable secure copy server** (Activer le serveur Secure Copy).

Étape 8 Cliquez sur **Apply** (Appliquer).

Exemples

L'exemple suivant montre une session SCP vers l'ASA. À partir d'un client sur l'hôte externe, effectuez un transfert de fichiers SCP. Par exemple, dans Linux, saisissez la commande suivante :

scp -v -pw *password* [*path*/]*source_filename*
*username@asa_address***:** {**disk0**|**disk1**}**:/**[*path*/]*dest_filename*

L'option **-v** correspond à verbose (détaillé), et si **-pw** n'est pas spécifié, vous serez invité à saisir un mot de passe.

Configurer SSH pour l'accès par mot de passe

Configurez l'authentification SSH à l'aide d'un nom d'utilisateur et d'un mot de passe.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authentication (Authentification)**.

Étape 2 Cochez la case **SSH**.

Étape 3 Choisissez la base de données **LOCALE** ou un serveur AAA dans la liste déroulante **Server Group** (Groupe de serveurs).

Ce paramètre n'affecte pas l'authentification par clé publique locale pour les noms d'utilisateur qui ont une clé publique configurée. L'ASA utilise implicitement la base de données locale pour l'authentification par clé publique. Ce paramètre n'affecte que les noms d'utilisateur locaux avec mots de passe. Si vous souhaitez autoriser l'authentification par clé publique ou l'utilisation du mot de passe par un utilisateur local, vous devez configurer explicitement l'authentification locale à l'aide de ce paramètre pour autoriser l'accès par mot de passe.

Étape 4 Cliquez sur **Apply** (Appliquer).

Étape 5 Créez un utilisateur dans la base de données locale ou sur un serveur AAA qui peut être utilisé pour l'accès SSH. Consultez la procédure suivante pour ajouter un nom d'utilisateur local (conseillé).

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add User Account-Identity** (Ajouter une identité de compte d'utilisateur) apparaît.

b) Entrez un nom d'utilisateur et un mot de passe, puis confirmez le mot de passe.

Vous pouvez utiliser l'authentification par clé publique ou l'authentification par mot de passe pour le même utilisateur local. L'authentification par clé publique n'est pas prise en charge par un serveur AAA.

c) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Étape 6 Générez une paire de clés (pour les ASA physiques uniquement).

Pour l'ASAv, les paires de clés sont automatiquement créées après le déploiement. L'ASAv ne prend en charge que la clé RSA.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)**.
b) Cliquez sur **Add** (Ajouter), puis sur le bouton radio **Add a new identity certificate** (Ajouter un nouveau certificat d'identité).
c) Cliquez sur **New** (Nouveau).
d) Dans la boîte de dialogue **Add Key Pair** (Ajouter une paire de clés), précisez le type et la taille, puis cliquez sur **Generate Now** (Générer maintenant).

La paire de clés par défaut utilisée est EdDSA, ECDSAA, puis RSA. Pour RSA, choisissez une taille de 2048 bits ou plus.

Vous pouvez ensuite **annuler** dans la boîte de dialogue du certificat, car vous souhaitiez uniquement générer la paire de clés.



Remarque EdDSA n'est pas pris en charge avec la pile CiscoSSH.

e) Cliquez sur **Apply** (Appliquer).

Configurer SSH pour l'accès par clé publique

Configurez l'authentification SSH à l'aide d'une clé publique.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.

Procédure

Étape 1 Créez un utilisateur dans la base de données locale qui peut être utilisé pour l'accès SSH.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add User Account-Identity** (Ajouter une identité de compte d'utilisateur) apparaît.

b) Entrez un nom d'utilisateur et un mot de passe, puis confirmez le mot de passe.

Vous pouvez créer un utilisateur sans mot de passe si vous souhaitez forcer l'utilisateur à utiliser l'authentification par clé publique au lieu de l'authentification par mot de passe. Si vous configurez l'authentification par clé publique ainsi qu'un mot de passe, l'utilisateur peut se connecter en utilisant l'une ou l'autre des méthodes si vous configurez explicitement l'authentification AAA dans cette procédure.

c) Activez l'authentification par clé publique. Choisissez l'un des volets suivants :

- **Public Key Authentication** (Authentification par clé publique) : collez une clé publique codée en Base64. Vous pouvez générer la clé à l'aide de n'importe quel logiciel de génération de clés SSH (comme ssh keygen) qui peut générer des clés brutes ssh-rsa, ssh-ed25519 ou ecdsa-sha2-nistp (sans certificats). Lorsque vous affichez une clé existante, la clé est chiffrée à l'aide d'un hachage SHA-256. Si vous devez copier et coller une clé de hachage, cochez la case **Key is hashed** (La clé est hachée).

  Pour supprimer une clé d'authentification, cliquez sur **Delete Key** (Supprimer la clé) pour afficher une boîte de dialogue de confirmation. Cliquez sur **Yes** (Oui) pour supprimer la clé d'authentification ou sur **No** (Non) pour la conserver.

- **Public Key Using PKF** (Clé publique utilisant PKF) : cochez la case **Specify a new PKF** (Spécifier une nouvelle clé PKF), et collez ou importez une clé formatée de fichier de clé publique (PKF), jusqu'à 4 096 bits. Utilisez ce format pour les clés trop importantes pour les coller au format base64. Par exemple, vous pouvez générer une clé de 4 096 bits à l'aide de ssh keygen, puis la convertir en PKF, et l'importer dans ce volet. Lorsque vous affichez une clé existante, celle-ci est chiffrée à l'aide du hachage SHA-256. Si vous devez copier et coller une clé de hachage, copiez-la à partir du volet **Public Key Authentication** (Authentification de clé publique) et collez-la dans ce volet sur le nouvel ASA avec la case **Key is hashed** (La clé de hachage) cochée.

  Pour supprimer une clé d'authentification, cliquez sur **Delete Key** (Supprimer la clé) pour afficher une boîte de dialogue de confirmation. Cliquez sur **Yes** (Oui) pour supprimer la clé d'authentification ou sur **No** (Non) pour la conserver.

d) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Étape 2 Générez une paire de clés (pour les ASA physiques uniquement).

Pour l'ASAv, les paires de clés sont automatiquement créées après le déploiement. L'ASAv ne prend en charge que la clé RSA.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)**.
b) Cliquez sur **Add** (Ajouter), puis sur le bouton radio **Add a new identity certificate** (Ajouter un nouveau certificat d'identité).
c) Cliquez sur **New** (Nouveau).
d) Dans la boîte de dialogue **Add Key Pair** (Ajouter une paire de clés), précisez le type et la taille, puis cliquez sur **Generate Now** (Générer maintenant).

   La paire de clés par défaut utilisée est EdDSA, ECDSAA, puis RSA. Pour RSA, choisissez une taille de 2048 bits ou plus.

Remarque Avec la pile CiscoSSH, seule la paire de clés configurée est partagée par l'ASA au moment de l'établissement d'une connexion.

Vous pouvez ensuite **annuler** dans la boîte de dialogue du certificat, car vous souhaitiez uniquement générer la paire de clés.

Remarque EdDSA n'est pas pris en charge avec la pile CiscoSSH.

e) Cliquez sur **Apply** (Appliquer).

Exemples

L'exemple suivant montre comment s'authentifier à l'aide d'une clé au format PKF :

L'exemple suivant génère une clé partagée pour SSH sur un système Linux ou Macintosh et l'importe dans l'ASA :

1. Générez les clés publiques et privées RSA pour 4 096 bits sur votre ordinateur :

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
```

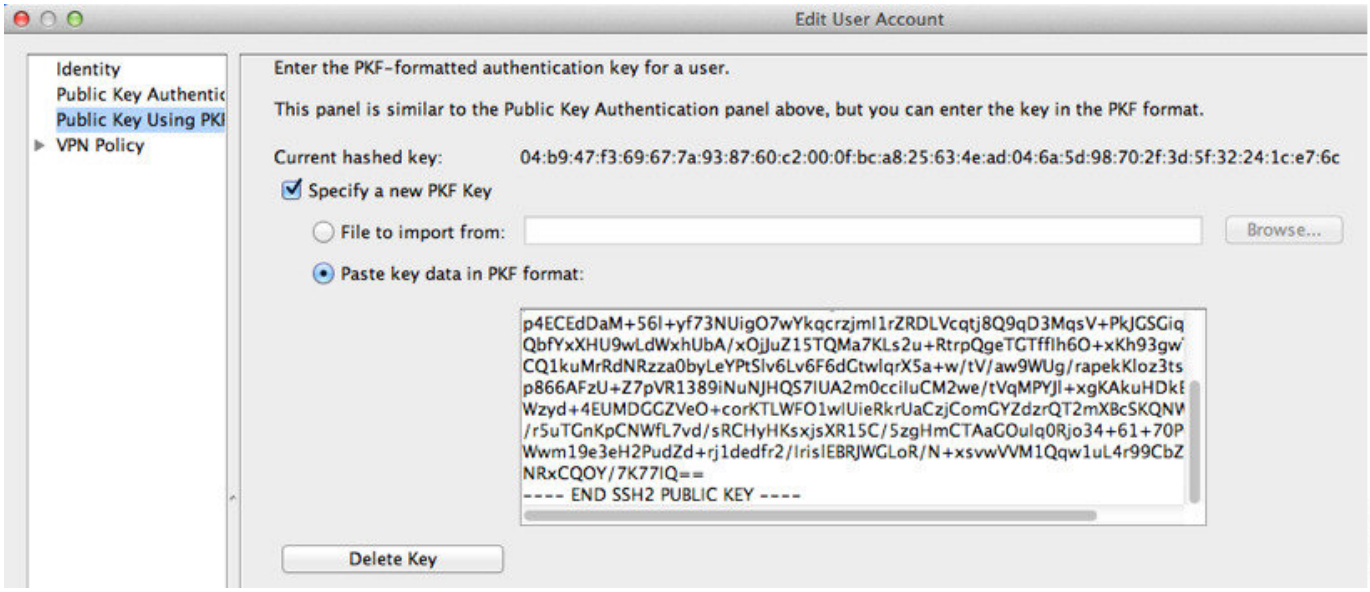
```
|  o o            |
| ooooo           |
+-----------------+
```

2. Convertissez la clé au format PKF :

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by john@jcrichton-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3. Copiez la clé dans votre presse-papiers.

4. Dans ASDM, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)**, sélectionnez le nom d'utilisateur, puis cliquez sur **Edit** (Modifier). Cliquez sur **Public Key Using PKF** (Clé publique utilisant PKF) et collez la clé dans la fenêtre :



5. Vérifiez que l'utilisateur peut se connecter par SSH à l'ASA. Pour le mot de passe, saisissez le mot de passe de la clé SSH que vous avez spécifié lors de la création de la paire de clés.

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
```

```
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

La boîte de dialogue suivante s'affiche pour que vous puissiez saisir votre phrase secrète :



Pendant ce temps, dans la session de terminal :

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

Configurer l'accès Telnet

Cette section décrit comment configurer l'accès ASA pour Telnet. Vous ne pouvez pas utiliser Telnet sur l'interface de sécurité la plus basse, sauf si vous utilisez Telnet dans un tunnel VPN.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.
- Pour accéder à l'interface de ligne de commande d'ASA à l'aide de Telnet, saisissez le mot de passe de connexion. Vous devez définir manuellement le mot de passe avant d'utiliser Telnet.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue**Add Device Access Configuration** (Ajouter une configuration d'accès à l'appareil) apparaît.

Étape 2 Choisissez **Telnet**.

Étape 3 Choisissez l'interface de gestion et définissez les adresses IP d'hôte autorisées, puis cliquez sur **OK**.

Spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 1148), spécifiez l'interface BVI nommée.

Étape 4 (Facultatif) Définissez le **Telnet Timeout** (Délai d'expiration Telnet). La valeur de délai d'expiration par défaut est de 5 minutes.

Étape 5 Cliquez sur **Apply** (Appliquer).

Étape 6 Définissez un mot de passe de connexion avant de pouvoir vous connecter à Telnet; il n'y a pas de mot de passe par défaut.

a) Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)**.
b) Cochez la case **Change the password to access the console of the security appliance** (Changer le mot de passe pour accéder à la console de l'appareil de sécurité) dans la zone **Telnet Password** (Mot de passe Telnet).
c) Entrez l'ancien mot de passe (laissez ce champ vide pour un nouvel ASA), puis entrez le nouveau mot de passe et confirmez-le.
d) Cliquez sur **Apply** (Appliquer).

Configurer la redirection HTTP pour l'accès ASDM ou le SSL VPN sans client

Vous devez utiliser HTTPS pour vous connecter à l'ASA à l'aide d'ASDM ou du SSL VPN sans client. Pour plus de commodité, vous pouvez rediriger les connexions de gestion HTTP vers HTTPS. Par exemple, en redirigeant HTTP, vous pouvez saisir **http://10.1.8.4/admin/** ou **https://10.1.8.4/admin/** et arriver toujours à la page de lancement d'ASDM à l'adresse HTTPS.

Vous pouvez rediriger le trafic IPv4 et IPv6.

Avant de commencer

Normalement, vous n'avez pas besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Cependant, pour la redirection HTTP, vous devez activer un critère d'accès pour autoriser HTTP; sinon, l'interface ne peut pas être à l'écoute du port HTTP.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **HTTP Redirect (Redirection HTTP)**.

Le tableau affiche les interfaces actuellement configurées et si la redirection est activée sur une interface.

Étape 2 Sélectionnez l'interface que vous utilisez pour ASDM et cliquez sur **Edit** (Modifier).

Étape 3 Configurez les options suivantes dans la boîte de dialogue **Edit HTTP/HTTPS Settings** (Modifier les paramètres HTTP/HTTPS) :

- **Redirect HTTP to HTTPS** (Rediriger les requêtes HTTP vers HTTPS) : redirige les requêtes HTTP vers HTTPS.

- **HTTP Port** (Port HTTP) : identifie le port à partir duquel l'interface redirige les connexions HTTP. La valeur par défaut est 80.

Étape 4 Cliquez sur **OK**.

Configurer l'accès de gestion sur un tunnel VPN

Si votre tunnel VPN se termine sur une interface, mais que vous souhaitez gérer l'ASA en accédant à une autre interface, vous devez identifier cette interface comme une interface d'accès de gestion. Par exemple, si vous saisissez l'ASA à partir de l'interface externe, cette fonctionnalité vous permet de vous connecter à l'interface interne à l'aide d'ASDM, SSH, ou Telnet; ou vous pouvez envoyer un message Ping à l'interface interne en entrant à partir de l'interface externe.

Remarque Cette fonctionnalité n'est pas prise en charge pour SSH si vous utilisez la pile CiscoSSH, qui est la valeur par défaut.

Remarque Cette fonctionnalité n'est pas prise en charge pour SNMP. Pour SNMP sur VPN, nous vous recommandons d'activer SNMP sur une interface de boucle avec retour. Vous n'avez pas besoin d'activer la fonctionnalité d'accès de gestion pour utiliser SNMP sur l'interface de boucle avec retour. La boucle avec retour fonctionne également pour SSH.

L'accès VPN à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre accès VPN se trouve sur l'interface externe, vous pouvez uniquement initier une connexion directement à l'interface externe. Vous devez activer le VPN sur l'interface directement accessible de l'ASA et utiliser la résolution de noms pour ne pas avoir à vous souvenir de plusieurs adresses.

L'accès de gestion est disponible par les types de tunnel VPN suivants : clients IPsec, IPsec de site à site, Easy VPN et le SSL VPN Secure Client (services client sécurisés).

Avant de commencer

- Cette fonctionnalité n'est pas prise en charge sur les interfaces de gestion uniquement.
- Lorsque vous utilisez une interface d'accès de gestion et que vous configurez la NAT d'identité, vous devez configurer la NAT avec l'option de recherche de routage. Pour en savoir plus, consultez la section « Accès à la gestion de la NAT et du VPN » dans le chapitre *Exemples de NAT et référence* dans la version appropriée du Guide de configuration de l'interface de ligne de commande du pare-feu ASA.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Management Interface (Interface de gestion)**.

Étape 2 Choisissez l'interface ayant la sécurité la plus élevée (l'interface interne) dans la liste déroulante **Management Access Interface** (Interface d'accès de gestion).

Pour Site à site, vous pouvez spécifier une BVI nommée (en mode routé).

Étape 3 Cliquez sur **Apply** (Appliquer).

L'interface de gestion est attribuée et la modification est enregistrée dans la configuration d'exécution.

Configurer l'accès de gestion pour FXOS sur les interfaces de données en mode plateforme Firepower 2100

Si vous souhaitez gérer FXOS sur le Firepower 2100 en mode plateforme à partir d'une interface de données, vous pouvez configurer l'accès SSH, HTTPS et SNMP. Cette fonctionnalité est utile si vous souhaitez gérer le périphérique à distance, mais que vous souhaitez conserver la gestion 1/1, qui est la méthode d'accès native à FXOS, sur un réseau isolé. Si vous activez cette fonctionnalité, vous pouvez continuer à utiliser l'interface de gestion Management 1/1 pour l'accès local uniquement. Cependant, vous ne pouvez pas autoriser l'accès *à distance* depuis ou vers l'interface de gestion Management 1/1 pour FXOS en même temps que l'utilisation de cette fonctionnalité. Cette fonctionnalité nécessite le transfert du trafic vers les interfaces de données ASA à l'aide d'un chemin interne (valeur par défaut), et vous ne pouvez spécifier qu'une seule passerelle de gestion FXOS.

L'ASA utilise des ports non standard pour l'accès FXOS; le port standard est réservé à l'utilisation par l'ASA sur la même interface. Lorsque l'ASA transfère le trafic vers FXOS, il traduit le port de destination non standard en port FXOS pour chaque protocole (ne modifiez pas le port HTTPS dans FXOS). L'adresse IP de destination du paquet (qui est l'adresse IP de l'interface ASA) est également convertie en une adresse interne pour l'utilisation par FXOS. L'adresse source reste inchangée. Pour renvoyer le trafic, l'ASA utilise sa table de routage de données pour déterminer la bonne interface de sortie. Lorsque vous accédez à l'adresse IP de données ASA pour l'application de gestion, vous devez vous connecter en utilisant un nom d'utilisateur FXOS; les noms d'utilisateur ASA ne s'appliquent qu'à l'accès de gestion ASA.

Vous pouvez également activer l'*initiation* du trafic de gestion FXOS sur les interfaces de données ASA. Cette fonction est requise pour les alertes SNMP ou pour l'accès au serveur NTP et DNS, par exemple. Par défaut, l'initiation du trafic de gestion FXOS est activée pour l'interface externe ASA pour la communication avec les serveurs DNS et NTP (cette fonctionnalité est requise pour la communication avec les licences Smart).

Avant de commencer

- Mode contexte unique seulement.
- Exclut les interfaces de gestion ASA uniquement.
- Vous ne pouvez pas utiliser un tunnel VPN pour l'interface de données ASA et accéder directement à FXOS. Comme solution de contournement pour SSH, vous pouvez faire appel au VPN vers l'ASA, accéder à l'interface de ligne de commande de l'*ASA*, puis utiliser la commande **connect fxos** pour accéder à l'interface de ligne de commande de FXOS. Notez que SSH, HTTPS et SNMPv3 sont/peuvent être chiffrés, de sorte qu'une connexion directe à l'interface de données est sécurisée.
- Assurez-vous que la passerelle FXOS est configurée pour acheminer le trafic vers les interfaces de données ASA (par défaut). Consultez le guide de démarrage pour en savoir plus sur la configuration de la passerelle.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **FXOS Remote Management (Gestion à distance FXOS)**.

Étape 2 Activez la gestion à distance FXOS.

a) Choisissez **HTTPS**, **SNMP** ou **SSH** dans le volet de navigation.

b) Cliquez sur **Add** (ajouter) et définissez l'**interface** sur laquelle vous souhaitez autoriser la gestion, définissez l'adresse IP (**IP Address**) autorisée pour la connexion, puis cliquez sur **OK**.

Vous pouvez créer plusieurs entrées pour chaque type de protocole. Définissez le **port** si vous ne souhaitez pas utiliser les paramètres par défaut suivants :

- Port HTTPS par défaut : 3443
- Port SNMP par défaut : 3061
- Port SSH par défaut : 3022

Étape 3 Permettez à FXOS d'initier des connexions de gestion à partir de l'interface ASA.

a) Choisissez **FXOS Traffic Initiation** (initialisation du trafic FXOS) dans le volet de navigation.

b) Cliquez sur **Add** et activez les interfaces ASA par lesquelles vous devez envoyer le trafic de gestion FXOS. Par défaut, l'interface externe est activée.

Étape 4 Cliquez sur **Apply** (Appliquer).

Étape 5 Connectez-vous à Firewall Chassis Manager sur l'interface de gestion Management 1/1 (par défaut https://192.168.45.45, avec le nom d'utilisateur : **admin** et le mot de passe : **Admin123**).

Étape 6 Cliquez sur l'onglet **Platform Settings** (paramètres de plateforme) et activez **SSH**, **HTTPS** ou **SNMP**.

SSH et HTTPS sont activés par défaut.

Étape 7 Configurez une liste d'accès (**Access List**) dans l'onglet des paramètres de la plateforme (**Platform Settings**) pour autoriser vos adresses de gestion. SSH et HTTPS autorisent uniquement le réseau de gestion Management 1/1 192.168.45.0 par défaut. Vous devez autoriser toutes les adresses que vous avez spécifiées dans la configuration de gestion à distance FXOS (**FXOS Remote Management**) sur l'ASA.

Modifier le délai d'expiration de la console

Le délai d'expiration de la console définit combien de temps une connexion peut rester en mode d'exécution privilégié ou en mode de configuration; une fois le délai d'expiration atteint, la session passe en mode EXEC de l'utilisateur. Par défaut, la session n'expire pas. Ce paramètre n'a pas d'incidence sur la durée de votre connexion au port de console, qui n'expire jamais.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Command Line (CLI) (Ligne de commande (interface de ligne de commande))** > **Console Timeout (Délai d'expiration de la console)**.

Étape 2 Définissez une nouvelle valeur de délai d'expiration en minutes. Pour spécifier une durée illimitée, saisissez **0**. La valeur par défaut est 0.

Étape 3 Cliquez sur **Apply** (Appliquer).

La modification de la valeur du délai d'expiration est enregistrée dans la configuration en cours d'exécution.

Personnaliser une invite de l'interface de ligne de commande

La possibilité d'ajouter des renseignements à une invite vous permet de voir en un coup d'œil à quel ASA vous êtes connecté lorsque vous avez plusieurs modules. Lors d'un basculement, cette fonctionnalité est utile lorsque les deux ASA ont le même nom d'hôte.

En mode de contexte multiple, vous pouvez afficher l'invite étendue lorsque vous vous connectez à l'espace d'exécution du système ou au contexte d'administration. Dans un contexte de non-administration, vous ne voyez que l'invite par défaut, qui est le nom d'hôte et le nom de contexte.

Par défaut, l'invite affiche le nom d'hôte de l'ASA. En mode de contexte multiple, l'invite affiche également le nom du contexte. Vous pouvez afficher les éléments suivants dans l'invite de l'interface de ligne de commande :

cluster-unit	Affiche le nom de l'unité de grappe. Chaque unité d'une grappe peut avoir un nom unique.
context	(Mode multiple uniquement) Affiche le nom du contexte actuel.
domaine	Affiche le nom de domaine.
hostname	Affiche le nom d'hôte.
priority	Affiche la priorité de basculement comme pri (principal) ou sec (secondaire).

state	Affiche l'état de transmission du trafic ou le rôle de l'unité. Pour le basculement, les valeurs suivantes sont affichées pour le mot clé d'état : • **act** : le basculement est activé et l'unité transmet activement le trafic. • **stby** : le basculement est activé et l'unité ne transmet pas de trafic et est en veille, en panne ou dans un autre état non actif. • **actNoFailover** : le basculement n'est pas activé et l'unité transmet activement le trafic. • **stbyNoFailover** : le basculement n'est pas activé et l'unité ne transmet pas de trafic. Cela pourrait se produire en cas de défaillance d'interface au-dessus du seuil sur l'unité en veille. Pour la mise en grappe, les valeurs du contrôle et des données sont affichées.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Command Line (CLI) (Ligne de commande (interface de ligne de commande))** > **CLI Prompt (Invite de l'interface de ligne de commande).**

Étape 2 Effectuez l'une des opérations suivantes pour personnaliser l'invite :

- Cliquez sur l'attribut dans la liste **Available Prompts** (Invites disponibles), puis cliquez sur **Add** (Ajouter). Vous pouvez ajouter plusieurs attributs à l'invite. L'attribut est déplacé de la liste **Available Prompts** (Invites disponibles) vers la liste **Selected Prompts** (Invites sélectionnées).
- Cliquez sur l'attribut dans la liste **Selected Prompts** (Invites sélectionnées), puis cliquez sur **Delete** (Supprimer). L'attribut est déplacé de la liste **Selected Prompts** (Invites sélectionnées) vers la liste **Available Prompts** (Invites disponibles).
- Cliquez sur l'attribut dans la liste **Selected Prompts** (Invites sélectionnées), puis sur **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas) pour modifier l'ordre dans lequel les attributs s'affichent.

L'invite est modifiée et s'affiche dans le champ **CLI Prompt Preview** (Aperçu de l'invite de l'interface de ligne de commande).

Étape 3 Cliquez sur **Apply**.

La nouvelle invite est enregistrée dans la configuration d'exécution.

Configurer une bannière de connexion

Vous pouvez configurer un message pour qu'il s'affiche lorsqu'un utilisateur se connecte à l'ASA, avant qu'un utilisateur ne se connecte ou avant qu'un utilisateur n'entre en mode d'exécution privilégié.

- Du point de vue de la sécurité, il est important que votre bannière dissuade les accès non autorisés. N'utilisez pas les mots « bienvenue » ou « s'il vous plaît », car ils semblent inviter des intrus à entrer. La bannière suivante donne le bon ton en cas d'accès non autorisé :

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- Après l'ajout d'une bannière, les sessions Telnet ou SSH à l'ASA peuvent se fermer si :
  - La mémoire système est insuffisante pour traiter les messages sur bannière.
  - Une erreur d'écriture TCP se produit lors de la tentative d'affichage des messages sur bannière.
- Consultez la RFC 2196 pour connaître les lignes directrices relatives aux messages sur bannière.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Command Line (CLI) (Ligne de commande (interface de ligne de commande))** > **Banner (Bannière)**.

Étape 2 Ajoutez le texte de votre bannière dans le champ du type de bannière que vous créez pour l'interface de ligne de commande :

- La bannière de session (exec) apparaît lorsqu'un utilisateur accède au mode d'exécution privilégié au niveau de l'interface de ligne de commande.
- La bannière de connexion apparaît lorsqu'un utilisateur se connecte à l'interface de ligne de commande.
- La bannière du message du jour (motd) s'affiche lorsqu'un utilisateur se connecte à l'interface de ligne de commande pour la première fois.
- La bannière ASDM apparaît lorsqu'un utilisateur se connecte à ASDM, après son authentification. L'utilisateur dispose de deux options pour ignorer la bannière :
  - **Continue** (Continuer) : ignorer la bannière et terminer la connexion.
  - **Disconnect** (Se déconnecter) : ignorer la bannière et terminer la connexion.
- Seuls les caractères ASCII sont autorisés, y compris une nouvelle ligne (Entrée), qui compte comme deux caractères.
- N'utilisez pas les onglets dans la bannière, car ils ne sont pas conservés dans la version de l'interface de ligne de commande.
- Il n'y a aucune limite de longueur pour les bannières autres que celles de la RAM et de la mémoire flash.
- Vous pouvez ajouter de manière dynamique le nom d'hôte ou le nom de domaine de l'ASA en incluant les chaînes **$(hostname)** et **$(domain)**.
- Si vous configurez une bannière dans la configuration système, vous pouvez utiliser ce texte de bannière dans un contexte en utilisant la chaîne **$(system)** dans la configuration du contexte.

Étape 3 Cliquez sur **Apply** (Appliquer).

La nouvelle bannière est enregistrée dans la configuration d'exécution.

Définir un quota de sessions de gestion

Vous pouvez établir un nombre maximum de sessions ASDM, SSH et Telnet simultanées qui sont autorisées sur l'ASA. Si le maximum est atteint, aucune session supplémentaire n'est autorisée et un message de journal système est généré. Pour empêcher un verrouillage du système, le mécanisme de quota de sessions de gestion ne peut pas bloquer une session de console.



Remarque En mode de contexte multiple, vous ne pouvez pas configurer le nombre de sessions ASDM, où le maximum est fixe à 5 sessions.



Remarque Si vous définissez également une limite de ressources par contexte pour le nombre maximum de sessions administratives (SSH, etc.), la valeur la plus basse sera utilisée.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration** > **Device List (Liste des périphériques)**, cliquez deux fois sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Management Session Quota (Quota de sessions de gestion)**

Étape 2 Saisissez le nombre maximum de sessions simultanées.

- **Aggregate** (Agrégé) : définit le nombre agrégé de sessions entre 1 et 15. La valeur par défaut est de 15.
- **HTTP Sessions** (Sessions HTTP) : définit le nombre maximum de sessions HTTPS (ASDM), entre 1 et 5. La valeur par défaut est égale à 5.
- **SSH Sessions** (Sessions SSH) : définit le nombre maximum de sessions SSH, entre 1 et 5. La valeur par défaut est égale à 5.
- **Telnet Sessions** (Sessions Telnet) : définit le nombre maximum de sessions Telnet, entre 1 et 5. La valeur par défaut est égale à 5.
- **User Sessions** (Sessions d'utilisateur) : définit le nombre maximum de sessions par utilisateur, entre 1 et 5. La valeur par défaut est égale à 5.

Étape 3 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications de configuration.

Configurer AAA pour les administrateurs système

Cette section décrit comment configurer l'authentification, l'autorisation de gestion et l'autorisation de commande pour les administrateurs système.

Configurer l'authentification de gestion

Configurez l'authentification pour l'accès à l'interface de ligne de commande et à ASDM.

À propos de l'authentification de gestion

La façon dont vous vous connectez à l'ASA dépend de si vous activez ou non l'authentification.

À propos de l'authentification SSH

Consultez le comportement suivant pour l'accès SSH avec et sans authentification :

- Aucune authentification : SSH n'est pas disponible sans authentification.
- Authentification : lorsque vous activez l'authentification SSH, vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données locale des utilisateurs. Pour l'authentification par clé publique, l'ASA ne prend en charge que la base de données locale. Si vous configurez l'authentification par clé publique SSH, l'ASA utilise implicitement la base de données locale. Il vous suffit de configurer explicitement l'authentification SSH lorsque vous utilisez un nom d'utilisateur et un mot de passe pour vous connecter. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'authentification Telnet

Consultez le comportement suivant pour l'accès Telnet avec et sans authentification :

- Aucune authentification : si vous n'activez aucune authentification pour Telnet, vous ne saisissez pas de nom d'utilisateur; vous saisissez le mot de passe de connexion. Il n'y a pas de mot de passe par défaut, vous devez donc en définir un avant de pouvoir vous connecter à l'ASA via Telnet. Vous accédez au mode EXEC de l'utilisateur.
- Authentification : si vous activez l'authentification Telnet, vous saisissez le nom d'utilisateur et le mot de passe définis sur le serveur AAA ou la base de données des utilisateurs locale. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'authentification ASDM

Consultez le comportement suivant pour l'accès ASDM avec et sans authentification. Vous pouvez également configurer l'authentification par certificat, avec ou sans authentification AAA.

- Aucune authentification : par défaut, vous pouvez vous connecter à ASDM avec un nom d'utilisateur vide et le mot de passe d'activation, qui est vide par défaut. Nous vous suggérons de modifier le mot de passe d'activation dès que possible afin qu'il ne reste pas vide; voir Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet, à la page 759. Lorsque vous saisissez la commande **enable** au niveau de l'interface de ligne de commande pour la première fois, vous êtes invité

à modifier le mot de passe; ce comportement n'est pas appliqué lorsque vous vous connectez à ASDM. Notez que si vous saisissez un nom d'utilisateur et un mot de passe à l'écran de connexion (au lieu de laisser le nom d'utilisateur vide), ASDM vérifie la base de données locale à la recherche d'une correspondance.

- Authentification par certificat : (mode unique et routé uniquement) Vous pouvez exiger que l'utilisateur ait un certificat valide. Saisissez le nom d'utilisateur et le mot de passe du certificat pour que l'ASA valide le certificat par rapport au point de confiance PKI.
- Authentification AAA : lorsque vous activez l'authentification ASDM (HTTPS), vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données locale des utilisateurs. Vous ne pouvez plus utiliser ASDM avec un nom d'utilisateur vide et le mot de passe d'activation.
- Authentification AAA plus authentification par certificat : (mode unique et routé uniquement) Lorsque vous activez l'authentification ASDM (HTTPS), vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Si le nom d'utilisateur et le mot de passe sont différents pour l'authentification par certificat, vous êtes invité à les saisir également. Vous pouvez choisir de préremplir le nom d'utilisateur dérivé de votre certificat.

À propos de l'authentification série

Consultez le comportement suivant pour l'accès au port de console série avec et sans authentification :

- Aucune authentification : si vous n'activez aucune authentification pour l'accès en série, vous ne saisissez pas de nom d'utilisateur ni de mot de passe. Vous accédez au mode EXEC de l'utilisateur.
- Authentification : si vous activez l'authentification pour l'accès en série, vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'activation de l'authentification

Pour passer en mode d'exécution privilégié après la connexion, saisissez la commande **enable**. Le fonctionnement de cette commande dépend de si vous activez ou non l'authentification.

- Aucune authentification : si vous ne configurez pas l'authentification, saisissez le mot de passe d'activation du système lorsque vous saisissez la commande **enable**, qui est vide par défaut. La première fois que vous saisissez la commande **enable**, vous devez modifier le mot de passe. Cependant, si vous n'utilisez pas l'activation de l'authentification, après avoir saisi la commande **enable**, vous n'êtes plus connecté en tant qu'utilisateur particulier, ce qui peut affecter les fonctionnalités basées sur l'utilisateur telles que l'autorisation de commande. Pour conserver votre nom d'utilisateur, utilisez l'activation de l'authentification.
- Authentification : si vous configurez l'activation de l'authentification, l'ASA vous invite à entrer votre nom d'utilisateur et mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Cette fonctionnalité est particulièrement utile lorsque vous effectuez une autorisation de commande, dans laquelle les noms d'utilisateur sont importants pour déterminer les commandes qu'un utilisateur peut saisir.

Pour activer l'authentification à l'aide de la base de données locale, vous pouvez utiliser la commande **login** au lieu de la commande **enable**. La commande **login** conserve le nom d'utilisateur, mais ne nécessite aucune configuration pour activer l'authentification.

Mise en garde Si vous ajoutez à la base de données locale des utilisateurs qui peuvent accéder à l'interface de ligne de commande et que vous ne souhaitez pas entrer en mode d'exécution privilégié, vous devez configurer l'autorisation de commande. Sans autorisation de commande, les utilisateurs peuvent accéder au mode d'exécution privilégié (et à toutes les commandes) au niveau de l'interface de ligne de commande en utilisant leur propre mot de passe si leur niveau de privilège est de 2 ou plus (2 est la valeur par défaut). Vous pouvez également décourager l'utilisation de la commande login en utilisant un serveur AAA pour l'authentification au lieu de la base de données locale, ou vous pouvez définir tous les utilisateurs locaux au niveau 1 afin de pouvoir contrôler qui peut utiliser le mot de passe d'activation du système pour accéder au mode d'exécution privilégié.

Sessions du système d'exploitation hôte vers l'ASA

Certaines plateformes prennent en charge l'exécution de l'ASA en tant qu'application distincte : par exemple l'ASA sur le Firepower 4100/9300. Pour les sessions du système d'exploitation hôte à l'ASA, vous pouvez configurer l'authentification série et Telnet, selon le type de connexion. Par exemple, la commande **connect asa** dans FXOS sur le Firepower 2100 en mode plateforme utilise un port série.

En mode de contexte multiple, vous ne pouvez pas configurer de commandes AAA dans la configuration système. Cependant, si vous configurez l'authentification Telnet ou série dans le contexte d'administration, l'authentification s'applique également à ces sessions. Le serveur AAA du contexte d'administration ou la base de données locale des utilisateurs est utilisé dans cette instance.

Configurer l'authentification pour l'interface de ligne de commande ASDM et activer la commande Access

Avant de commencer

- Configurez l'accès Telnet, SSH ou HTTP.
- Pour l'authentification extérieure, configurez un groupe de serveurs AAA. Pour l'authentification locale, ajoutez des utilisateurs à la base de données locale.
- L'authentification de gestion HTTP ne prend pas en charge le protocole SDI pour un groupe de serveurs AAA.
- Cette fonctionnalité n'affecte pas l'authentification par clé publique SSH pour les noms d'utilisateur locaux avec la commande **ssh authentication**. L'ASA utilise implicitement la base de données locale pour l'authentification par clé publique. Cette fonctionnalité n'affecte que les noms d'utilisateur avec mots de passe. Si vous souhaitez autoriser l'authentification par clé publique ou l'utilisation du mot de passe par un utilisateur local, vous devez configurer explicitement l'authentification locale à l'aide de cette procédure pour autoriser l'accès par mot de passe.

Procédure

Étape 1 Pour authentifier les utilisateurs qui utilisent la commande **enable**, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authentication (Authentification)**, puis configurez les paramètres suivants :

a) Cochez la case **Enable** (activer).
b) Choisissez un nom de groupe de serveurs ou la base de données LOCAL.
c) (Facultatif) Si vous avez choisi un serveur AAA, vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Cochez la case **Use LOCAL when server group fails** (Utiliser LOCAL en cas d'échec du groupe de serveurs). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur AAA, car l'invite ASA n'indique pas quelle méthode est utilisée.

Étape 2 Pour authentifier les utilisateurs qui accèdent à l'interface de ligne de commande ou à ASDM, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authentication (Authentification)**, puis configurez les paramètres suivants :

a) Cochez une ou plusieurs des cases suivantes :

- **HTTP/ASDM** : authentifie le client ASDM qui accède à l'ASA à l'aide de HTTPS.
- **Serial** (Série) : authentifie les utilisateurs qui accèdent à l'ASA à l'aide du port de console. Pour Firepower 2100 en mode plateforme, ce mot clé affecte la console virtuelle accessible à partir de FXOS à l'aide de la commande **connect asa**.
- **SSH** : authentifie les utilisateurs qui accèdent à l'ASA à l'aide de SSH (mot de passe uniquement; l'authentification par clé publique utilise implicitement la base de données locale).
- **Telnet** : authentifie les utilisateurs qui accèdent à l'ASA à l'aide de Telnet.

b) Pour chaque service que vous avez vérifié, choisissez un nom de groupe de serveurs ou la base de données LOCAL.
c) (Facultatif) Si vous avez choisi un serveur AAA, vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Cochez la case **Use LOCAL when server group fails** (Utiliser LOCAL en cas d'échec du groupe de serveurs). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur AAA, car l'invite ASA n'indique pas quelle méthode est utilisée.

Étape 3 Cliquez sur **Apply** (Appliquer).

Contrôler l'interface de ligne de commande et l'accès ASDM avec l'autorisation de gestion

L'ASA vous permet de distinguer les utilisateurs administratifs et d'accès à distance lorsqu'ils s'authentifient. La différence des rôles d'utilisateur peut empêcher les utilisateurs du VPN d'accès à distance et de l'accès réseau d'établir une connexion administrative à l'ASA.

Avant de commencer

Utilisateurs RADIUS ou LDAP (mappés)

Lorsque les utilisateurs sont authentifiés par LDAP, les attributs LDAP natifs et leurs valeurs peuvent être mappés aux attributs ASA pour fournir des fonctionnalités d'autorisation spécifiques. Configurez Cisco VSA CVPN3000-Privilege-Level avec une valeur comprise entre 0 et 15, puis mappez les attributs LDAP à Cisco VAS CVPN3000-Privilege-Level.

L'attribut **service-type** IETF RADIUS, lorsqu'il est envoyé dans un message d'acceptation de l'accès à la suite d'une demande d'authentification et d'autorisation RADIUS, est utilisé pour désigner le type de service accordé à l'utilisateur authentifié.

L'attribut **privilege-level** RADIUS Cisco VSA (ID de fournisseur 3076, sous-ID 220), lorsqu'il est envoyé dans un message d'acceptation de l'accès, est utilisé pour désigner le niveau de privilège de l'utilisateur.

Utilisateurs TACACS+

L'autorisation est demandée par « service=shell », et le serveur répond par PASS (réussite) ou FAIL (échec).

Utilisateurs locaux

Configurez l'option **Access Restriction** (Restriction d'accès) pour un nom d'utilisateur donné. Par défaut, la restriction d'accès est **Full Access** (Accès complet), ce qui permet un accès complet à tous les services spécifiés par les options de l'onglet **Authentication** (Authentification).

Attributs d'autorisation de gestion

Consultez le tableau suivant pour connaître les types de serveurs AAA et les valeurs valides pour l'autorisation de gestion. L'ASA utilise ces valeurs pour déterminer le niveau d'accès de gestion.

Niveau de gestion	Attributs RADIUS/LDAP (mappés)	Attributs TACACS+	Attributs de la base de données locale
Accès complet : permet un accès complet à tous les services spécifiés par les commandes options de l'onglet **Authentication** (Authentification).	Type de service 6 (Administrateur), niveau de privilège 1	PASS (réussite), privilège de niveau 1	admin
Accès partiel : permet l'accès à l'interface de ligne de commande ou à ASDM lorsque vous configurez les commandes options de l'onglet **Authentication** (Authentification). Cependant, si vous configurez l'authentification **enable** avec la commande **Enable**, l'utilisateur de l'interface de ligne de commande ne peut pas accéder au mode d'exécution privilégié à l'aide de la commande **enable**.	Type de service 7 (invite NAS), niveau de privilège 2 et supérieur Les types de service Framed (2) et Login (1) sont traités de la même manière.	PASS (réussite), niveau de privilège 2 et supérieur	nas-prompt
Aucun accès : refuse l'accès de gestion. L'utilisateur ne peut pas utiliser les services spécifiés par les commandes options de l'onglet **Authentication** (Authentification) (à l'exception du mot clé **Serial** (Série); l'accès en série est autorisé). Les utilisateurs d'accès à distance (IPsec et SSL) peuvent toujours s'authentifier et mettre fin à leurs sessions d'accès à distance. Tous les autres types de services (voix, FAX, etc.) sont traités de la même manière.	Type de service 5 (sortant)	ÉCHEC	remote-access

Directives supplémentaires

- L'accès à la console de série n'est pas inclus dans l'autorisation de gestion.

- Vous devez également configurer l'authentification AAA pour l'accès de gestion afin d'utiliser cette fonctionnalité. Consultez Configurer l'authentification pour l'interface de ligne de commande ASDM et activer la commande Access, à la page 1157.
- Si vous utilisez l'authentification extérieure, vous devez préconfigurer un groupe de serveurs AAA avant d'activer cette fonctionnalité.
- L'autorisation HTTP est prise en charge uniquement en mode routé simple.

Procédure

Étape 1 Pour activer l'autorisation de gestion des sessions HTTP, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Autorisation)** et cochez la case **HTTP** dans la zone **Enable Authorization for ASA Command Access** (Activer l'autorisation pour l'accès à la commande ASA).

Remarque Pour configurer l'accès à la commande ASA, consultez Configurer l'autorisation de commande locale, à la page 1162.

Étape 2 Pour activer l'autorisation de gestion des sessions Telnet et SSH, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Autorisation)** et cochez la case **Enable** (Activer) dans la zone **Perform authorization for exec shell access** (Effectuer l'autorisation pour l'accès au shell d'exécution).

Étape 3 Sélectionnez les boutons radio **Remote** (Distant) ou **Local** afin de spécifier le serveur à utiliser pour l'autorisation de l'accès au shell d'exécution.

Étape 4 Pour activer l'autorisation de gestion, cochez la case **Allow privileged users to enter into EXEC mode on login** (Autoriser les utilisateurs privilégiés à entrer en mode EXEC lors de la connexion).

L'option **auto-enable** permet aux utilisateurs disposant d'un accès complet d'être placés directement en mode d'exécution privilégié. Sinon, les utilisateurs sont placés en mode EXEC utilisateur.

Configurer l'autorisation de commande

Si vous souhaitez contrôler l'accès aux commandes, l'ASA vous permet de configurer l'autorisation de commande, dans laquelle vous pouvez déterminer quelles commandes sont disponibles pour un utilisateur. Par défaut, lorsque vous vous connectez, vous pouvez accéder au mode EXEC de l'utilisateur, qui n'offre que des commandes minimales. Lorsque vous saisissez la commande **enable** (ou la commande **login** lorsque vous utilisez la base de données locale), vous pouvez accéder au mode d'exécution privilégié et aux commandes avancées, y compris les commandes de configuration.

Vous pouvez utiliser l'une des deux méthodes d'autorisation de commande suivantes :

- Niveaux de privilèges locaux
- Niveaux de privilèges du serveur TACACS+

À propos de l'autorisation de commande

Vous pouvez activer l'autorisation de commande pour que seuls les utilisateurs autorisés puissent saisir des commandes.

Méthodes d'autorisation de commande prises en charge

Vous pouvez utiliser l'une des deux méthodes d'autorisation de commande suivantes :

- Niveaux de privilèges locaux : configurez les niveaux de privilège de commande sur l'ASA. Lorsqu'un utilisateur local, RADIUS ou LDAP (si vous mappez des attributs LDAP aux attributs RADIUS) s'authentifie pour l'accès à l'interface de ligne de commande, l'ASA place cet utilisateur au niveau de privilège défini par la base de données locale, RADIUS ou le serveur LDAP. L'utilisateur peut accéder aux commandes au niveau de privilège attribué et en dessous. Notez que tous les utilisateurs accèdent au mode EXEC lorsqu'ils se connectent pour la première fois (commandes au niveau 0 ou 1). L'utilisateur doit s'authentifier de nouveau avec la commande **enable** pour accéder au mode d'exécution privilégié (commandes de niveau 2 ou supérieur), ou il peut se connecter avec la commande **login** (base de données locale uniquement).



Remarque Vous pouvez utiliser l'autorisation de commande locale sans aucun utilisateur dans la base de données locale et sans interface de ligne de commande ni authentification **enable**. Au lieu de cela, lorsque vous saisissez la commande **enable**, vous saisissez le mot de passe d'activation du système et l'ASA vous place au niveau 15. Vous pouvez ensuite créer des mots de passe d'activation pour chaque niveau, de sorte que lorsque vous entrez **enable** *n* (2 à 15), l'ASA vous place au niveau *n*. Ces niveaux ne sont pas utilisés, sauf si vous activez l'autorisation de commande locale.

- Niveaux de privilège du serveur TACACS+ : sur le serveur TACACS+, configurez les commandes qu'un utilisateur ou un groupe peut utiliser après s'être authentifié pour l'accès à l'interface de ligne de commande. Chaque commande qu'un utilisateur saisit au niveau de l'interface de ligne de commande est validée auprès du serveur TACACS+.

Contextes de sécurité et autorisation de commande

Les paramètres AAA sont distincts par contexte et ne sont pas partagés entre les contextes.

Lors de la configuration de l'autorisation de commande, vous devez configurer chaque contexte de sécurité séparément. Cette configuration vous offre la possibilité d'appliquer différentes autorisations de commande pour différents contextes de sécurité.

Lorsqu'ils passent d'un contexte de sécurité à l'autre, les administrateurs doivent savoir que les commandes autorisées pour le nom d'utilisateur spécifié lors de la connexion peuvent être différentes dans la nouvelle session de contexte ou que l'autorisation de commande peut ne pas être configurée du tout dans le nouveau contexte. Ne pas comprendre que les autorisations de commande peuvent différer d'un contexte de sécurité à l'autre peut dérouter un administrateur.



Remarque L'espace d'exécution du système ne prend pas en charge les commandes AAA; par conséquent, l'autorisation de commande n'est pas disponible dans l'espace d'exécution du système.

Niveaux de privilège de commande

Par défaut, les commandes suivantes sont affectées au niveau de privilège 0. Toutes les autres commandes sont affectées au niveau de privilège 15.

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

Si vous déplacez des commandes de mode de configuration à un niveau inférieur à 15, veillez également à déplacer la commande **configure** à ce niveau, sinon l'utilisateur ne pourra pas entrer en mode de configuration.

Configurer l'autorisation de commande locale

L'autorisation de commande locale vous permet d'affecter des commandes à l'un des 16 niveaux de privilège (0 à 15). Par défaut, chaque commande est affectée au niveau de privilège 0 ou 15. Vous pouvez définir chaque utilisateur comme étant à un niveau de privilège spécifique, et chaque utilisateur peut saisir n'importe quelle commande au niveau de privilège attribué ou en dessous. L'ASA prend en charge les niveaux de privilège d'utilisateur définis dans la base de données locale, un serveur RADIUS ou un serveur LDAP (si vous mappez des attributs LDAP aux attributs RADIUS).

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Autorisation)**.

Étape 2 Cochez la case **Enable authorization for ASA command access (Activer l'autorisation pour l'accès à la commande ASA)** > **Enable (Activer)**.

Étape 3 Choisissez **LOCAL** dans la liste déroulante **Server Group** (Groupe de serveurs).

Étape 4 Lorsque vous activez l'autorisation de commande locale, vous avez la possibilité d'attribuer manuellement les niveaux de privilège aux commandes individuelles ou à des groupes de commandes, ou d'activer les privilèges de compte d'utilisateur prédéfinis.

- Cliquez sur **Set ASDM Defined User Roles** (Définir les rôles d'utilisateur définis par ASDM) pour utiliser les privilèges de compte d'utilisateur prédéfinis.

La boîte de dialogue **ASDM Defined User Roles Setup** (Configuration des rôles d'utilisateur définis par ASDM) s'affiche. Cliquez sur **Yes** (Oui) pour utiliser les privilèges de compte d'utilisateur prédéfinis : **Admin** (niveau de privilège 15, avec accès complet à toutes les commandes de l'interface de ligne de commande); **Lecture seule** (niveau de privilège 5, avec accès en lecture seule); et **Affichage unquement** (niveau de privilège 3, avec accès à la section **de surveillance** seulement).

- Cliquez sur **Configure Command Privileges** (Configurer les privilèges de commande) pour configurer manuellement les niveaux de commande.

  La boîte de dialogue **Command Privileges Setup** (Configuration des privilèges de commande) apparaît. Vous pouvez afficher toutes les commandes en sélectionnant **All Modes** (Tous les modes) dans la liste déroulante **Command Mode** (Mode de commande), ou vous pouvez choisir un mode de configuration pour afficher les commandes disponibles dans ce mode. Par exemple, si vous choisissez contexte, vous pouvez afficher toutes les commandes disponibles en mode de configuration de contexte. Si une commande peut être saisie en mode EXEC de l'utilisateur ou en mode d'exécution privilégié ainsi qu'en mode de configuration et que la commande effectue des actions différentes dans chaque mode, vous pouvez définir le niveau de privilège pour ces modes séparément.

  La colonne **Variant** (Variante) affiche show, clear ou cmd. Vous pouvez définir les privilèges uniquement pour la forme show, clear ou configure de la commande. La forme configure de la commande est généralement la forme qui entraîne une modification de configuration, soit sous forme de commande non modifiée (sans le préfixe show ou clear), soit sous forme no (non).

  Pour modifier le niveau d'une commande, double-cliquez dessus ou cliquez sur **Edit** (Modifier). Vous pouvez définir le niveau entre 0 et 15. Vous pouvez uniquement configurer le niveau de privilège de la commande principale. Par exemple, vous pouvez configurer le niveau de toutes les commandes **aaa**, mais pas le niveau des commandes **aaa authentication** et **aaa authorization** séparément.

  Pour modifier le niveau de toutes les commandes qui s'affichent, cliquez sur **Select All** (Sélectionner tout), puis sur **Edit** (Modifier).

  Cliquez sur **OK** pour accepter vos modifications.

Étape 5 (Facultatif) Cochez la case **Perform authorization for exec shell access (Effectuer l'autorisation pour l'accès au shell d'exécution)** > **Enable (Activer)** afin d'activer les utilisateurs AAA pour l'autorisation de commande. Sans cette option, l'ASA ne prend en charge que les niveaux de privilège des utilisateurs de base de données locaux et définit par défaut tous les autres types d'utilisateurs au niveau 15.

Cette commande active également l'autorisation de gestion. Consultez Contrôler l'interface de ligne de commande et l'accès ASDM avec l'autorisation de gestion, à la page 1158.

Étape 6 Cliquez sur **Apply** (Appliquer).

Les paramètres d'autorisation sont affectés et les modifications sont enregistrées dans la configuration en cours d'exécution.

Configurer les commandes sur le serveur TACACS+

Vous pouvez configurer des commandes sur un serveur TACACS+ Cisco Secure Access Control Server (ACS) en tant que composant de profil partagé, pour un groupe ou pour des utilisateurs individuels. Pour les serveurs TACACS+ tiers, consultez la documentation de votre serveur pour en savoir plus sur la prise en charge des autorisations de commandes.

Consultez les lignes directrices suivantes pour la configuration des commandes dans Cisco Secure ACS version 3.1; la plupart de ces lignes directrices s'appliquent également aux serveurs tiers :

- L'ASA envoie les commandes à autoriser en tant que commandes shell; veuillez donc configurer les commandes sur le serveur TACACS+ en tant que commandes shell.

Remarque Cisco Secure ACS peut inclure un type de commande appelé « pix-shell ». N'utilisez pas ce type pour l'autorisation de commande ASA.

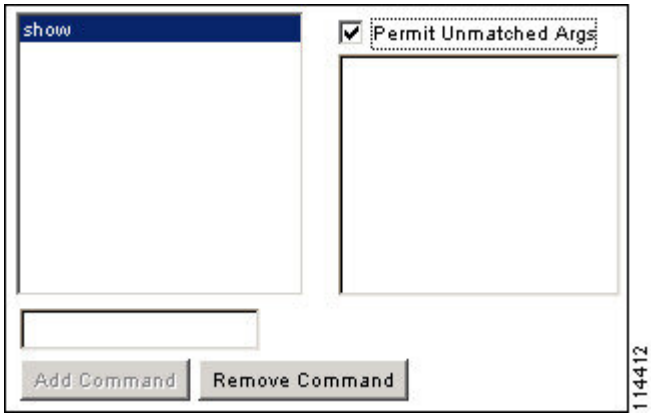
- Le premier mot de la commande est considéré comme la commande principale. Tous les mots supplémentaires sont considérés comme des arguments, qui doivent être précédés de **permit** ou **deny**.

  Par exemple, pour autoriser la commande **show running-configuration aaa-server**, ajoutez **show running-configuration** dans le champ de la commande et saisissez **permit aaa-server** dans le champ des arguments.

- Vous pouvez autoriser tous les arguments d'une commande que vous ne refusez pas explicitement en cochant la case **Permit Unmatched Args** (Autoriser les arguments sans correspondance).

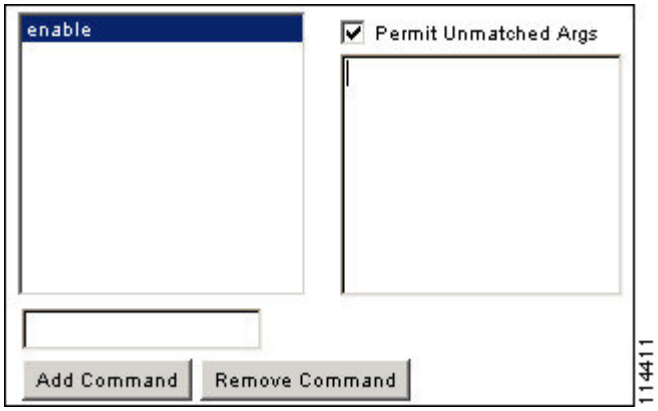
  Par exemple, vous pouvez configurer uniquement la commande **show**. Toutes les commandes **show** sont autorisées. Nous vous conseillons d'utiliser cette méthode pour que vous n'ayez pas à anticiper chaque variante d'une commande, y compris les abréviations et un point d'interrogation, qui indique l'utilisation de l'interface de ligne de commande (voir la figure suivante).

Illustration 89 : Autoriser toutes les commandes associées



- Pour les commandes composées d'un seul mot, vous *devez* autoriser des arguments sans correspondance, même s'il n'y a aucun argument pour la commande, par exemple **enable** ou **help** (voir la figure suivante).

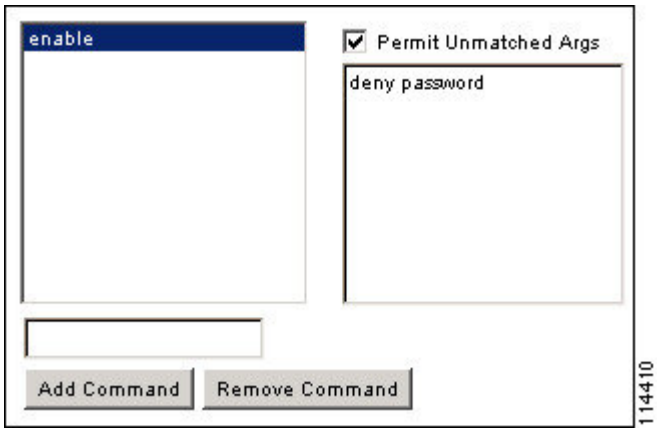
Illustration 90 : Autorisation des commandes à un seul mot



- Pour interdire certains arguments, entrez les arguments précédés de **deny**.

  Par exemple, pour autoriser **enable**, mais pas **enable password**, saisissez **enable** dans le champ des commandes et **deny password** dans le champ des arguments. Assurez-vous de cocher la case **Permit Unmatched Args** (Autoriser les arguments sans correspondance) pour que **enable** soit toujours autorisé (voir la figure suivante).

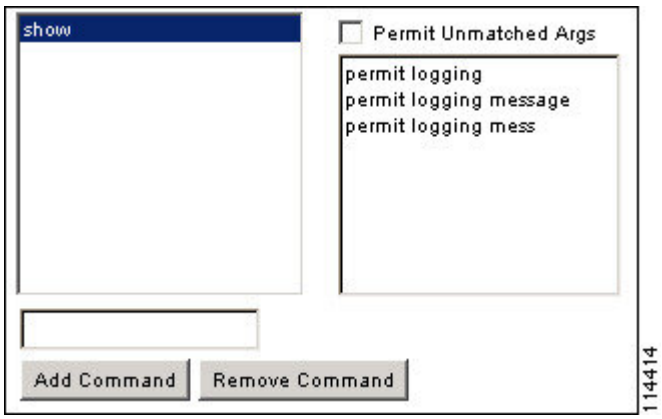
Illustration 91 : Interdire les arguments



- Lorsque vous abrégez une commande dans la ligne de commande, l'ASA développe le préfixe et la commande principale en texte intégral, mais envoie des arguments supplémentaires au serveur TACACS+ au fur et à mesure que vous les saisissez.

  Par exemple, si vous saisissez **sh log**, l'ASA envoie la commande complète au serveur TACACS+, **show logging**. Cependant, si vous saisissez **sh log mess**, l'ASA envoie **show logging mess** au serveur TACACS+, et non la commande étendue **show logging message**. Vous pouvez configurer plusieurs orthographes du même argument afin d'anticiper les abréviations (voir la figure suivante).

Illustration 92 : Spécifier les abréviations



- Nous vous conseillons d'autoriser les commandes de base suivantes pour tous les utilisateurs :
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**
  - **clear pager**
  - **quit**
  - **show version**

Configurer l'autorisation de commande TACACS+

Si vous activez l'autorisation de commande TACACS+ et qu'un utilisateur saisit une commande au niveau de l'interface de ligne de commande, l'ASA envoie la commande et le nom d'utilisateur au serveur TACACS+ pour déterminer si la commande est autorisée.

Avant d'activer l'autorisation de commande TACACS+, assurez-vous d'être connecté à l'ASA en tant qu'utilisateur défini sur le serveur TACACS+ et de disposer de l'autorisation de commande nécessaire pour continuer à configurer l'ASA. Par exemple, vous devez vous connecter en tant qu'utilisateur admin avec toutes les commandes autorisées. Sinon, vous pourriez vous retrouver involontairement bloqué.

N'enregistrez pas votre configuration avant d'être sûr qu'elle fonctionne comme vous le souhaitez. Si vous êtes bloqué par erreur, vous pouvez généralement récupérer l'accès en redémarrant l'ASA.

Assurez-vous que votre système TACACS+ est complètement stable et fiable. Le niveau de fiabilité nécessaire exige généralement que vous ayez un système de serveurs TACACS+ entièrement redondant et une connectivité entièrement redondante à l'ASA. Par exemple, dans votre ensemble de serveurs TACACS+, incluez un serveur connecté à l'interface 1 et un autre à l'interface 2. Vous pouvez également configurer l'autorisation de commande locale comme méthode de secours si le serveur TACACS+ n'est pas disponible.

Pour configurer l'autorisation de commande à l'aide d'un serveur TACACS+, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Autorisation)**

Étape 2 Cochez la case **Enable authorization for command access (Activer l'autorisation pour l'accès à la commande)** > **Enable (Activer)**.

Étape 3 Choisissez un nom de groupe de serveurs AAA dans la liste déroulante **Server Group** (Groupe de serveurs).

Étape 4 (Facultatif) Vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Pour ce faire, cochez la case **Use LOCAL when server group fails** (Utiliser LOCAL en cas d'échec du groupe de serveurs). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur AAA, car l'invite ASA n'indique pas quelle méthode est utilisée. Assurez-vous de configurer les utilisateurs dans la base de données locale et les niveaux de privilège de commande.

Étape 5 Cliquez sur **Apply** (Appliquer).

Les paramètres d'autorisation de commande sont affectés et les modifications sont enregistrées dans la configuration d'exécution.

Configurer une politique de mot de passe pour les utilisateurs de base de données locale

Lorsque vous configurez l'authentification pour l'accès à l'interface de ligne de commande ou à ASDM à l'aide de la base de données locale, vous pouvez configurer une politique de mot de passe qui oblige un utilisateur à changer de mot de passe après une durée spécifiée et qui exige également des normes de mot de passe tel qu'une longueur minimum et le nombre minimum de modifications de caractères.

La politique de mot de passe s'applique uniquement aux utilisateurs administratifs qui utilisent la base de données locale et non aux autres types de trafic qui peuvent utiliser la base de données locale, comme le VPN ou l'AAA pour l'accès au réseau, et non aux utilisateurs authentifiés par un serveur AAA.

Après avoir configuré la politique de mot de passe, lorsque vous modifiez un mot de passe (le vôtre ou celui d'un autre utilisateur), la politique de mot de passe s'applique au nouveau mot de passe. Tous les mots de passe existants sont conservés. La nouvelle politique s'applique à la modification du mot de passe avec la le volet **User Accounts** (Comptes d'utilisateurs) et la le volet **Change My Password** (Changer mon mot de passe).

Avant de commencer

- Configurez l'authentification AAA pour l'accès de l'interface de ligne de commande ou ASDM à l'aide de la base de données locale.
- Spécifiez les noms d'utilisateurs dans la base de données locale.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Password Policy (Politique de mot de passe)**.

Étape 2 Configurez n'importe quelle combinaison des options suivantes :

- **Minimum Password Length** (Longueur minimum du motde passe) : saisissez la longueur minimum des mots de passe. Les valeurs valides sont comprises entre 3 et 64 caractères. La longueur minimum conseillée du mot de passe est de 8 caractères.
- **Lifetime** (Durée de vie) : saisissez l'intervalle en jours après lequel les mots de passe expirent pour les utilisateurs distants (SSH, Telnet, HTTP); les utilisateurs au niveau du port de console ne sont jamais verrouillés en raison de l'expiration du mot de passe. Les valeurs valides sont comprises entre 0 et 65536 jours. La valeur par défaut est 0 jour, une valeur indiquant que les mots de passe n'expireront jamais.

  7 jours avant l'expiration du mot de passe, un message d'avertissement s'affiche. À l'expiration du mot de passe, l'accès au système est refusé aux utilisateurs distants. Pour y accéder après l'expiration, effectuez l'une des opérations suivantes :

  - Demandez à un autre administrateur de modifier votre mot de passe.
  - Connectez-vous au port de console physique pour modifier votre mot de passe.

- **Minimum Number Of** (Nombre minimum de) : spécifiez le nombre minimum de caractères parmi les types suivants :
  - **Numeric Characters** (Caractères numériques) : saisissez le nombre minimum de caractères numériques que les mots de passe doivent contenir. Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0.
  - **Lower Case Characters** (Caractères minuscules) : saisissez le nombre minimum de caractères minuscules que les mots de passe doivent contenir. Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0.
  - **Upper Case Characters** (Caractères majuscules) : saisissez le nombre minimum de caractères majuscules que les mots de passe doivent contenir. Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0.
  - **Special Characters** (Caractères spéciaux) : saisissez le nombre minimum de caractères spéciaux que les mots de passe doivent contenir. Les valeurs valides sont comprises entre 0 et 64 caractères. Les caractères spéciaux sont les suivants : !, @, #, $, %, ^, &, *, « (» et «) ». La valeur par défaut est 0.
  - **Different Characters from Previous Password** (Caractères différents du mot de passe précédent) : saisissez le nombre minimum de caractères que vous devez modifier entre l'ancien et le nouveau mot de passe. Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est

0. La correspondance des caractères est indépendante de la position, ce qui signifie que les caractères du nouveau mot de passe ne sont considérés comme modifiés que s'ils n'apparaissent nulle part dans le mot de passe actuel.

- **Enable Reuse Interval** (Activer l'intervalle de réutilisation) : vous pouvez interdire la réutilisation d'un mot de passe correspondant aux mots de passe utilisés précédemment, entre 2 et 7 mots de passe précédents. Les mots de passe précédents sont stockés dans la configuration sous chaque nom d'utilisateur sous forme chiffrée à l'aide de la commande **password-history**; cette commande n'est pas configurable par l'utilisateur.
- **Prevent Passwords from Matching Usernames** (Empêcher les mots de passe de correspondre aux noms d'utilisateurs) : interdisez un mot de passe qui correspond à un nom d'utilisateur.

Étape 3 (Facultatif) Cochez la case **Enable Password and Account Protection** (Activer la protection du mot de passe et du compte) pour demander aux utilisateurs de changer de mot de passe dans le volet **Change My Password** (Changer mon mot de passe) au lieu du volet **User Accounts** (Comptes d'utilisateurs). Le paramètre par défaut est désactivé : un utilisateur peut utiliser l'une ou l'autre des méthodes pour modifier son mot de passe.

Si vous activez cette fonctionnalité et essayez de changer votre mot de passe dans le volet **User Accounts** (Comptes d'utilisateurs), le message d'erreur suivant est généré :

```
ERROR: Changing your own password is prohibited
```

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer les paramètres de configuration.

Changer votre mot de passe

Si vous configurez une durée de validité du mot de passe dans la politique de mot de passe, vous devez changer votre mot de passe lorsque l'ancien mot de passe expire. Cette méthode de modification du mot de passe est requise si vous activez l'authentification par politique de mot de passe. Si l'authentification par politique de mot de passe n'est pas activée, vous pouvez utiliser cette méthode ou vous pouvez modifier directement votre compte d'utilisateur.

Pour modifier votre mot de passe d'utilisateur, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Change Password (Modifier le mot de passe)**.

Étape 2 Saisissez votre ancien mot de passe.

Étape 3 Saisissez votre nouveau mot de passe.

Étape 4 Confirmez votre nouveau mot de passe.

Étape 5 Cliquez sur **Make Change** (Appliquer la modification).

Étape 6 Cliquez sur l'icône **Save** (Enregistrer) pour enregistrer vos modifications dans la configuration en cours d'exécution.

Activer et afficher l'historique de connexion

Par défaut, l'historique de connexion est enregistré pendant 90 jours. Vous pouvez désactiver cette fonctionnalité ou modifier la durée, jusqu'à 365 jours.

Avant de commencer

- L'historique de connexion n'est enregistré que par unité; dans les environnements de basculement et de mise en grappe, chaque unité conserve uniquement son propre historique de connexion.
- Les données de l'historique de connexion ne sont pas conservées pendant les rechargements.
- Cette fonctionnalité s'applique aux noms d'utilisateur dans la base de données locale ou à partir d'un serveur AAA lorsque vous activez l'authentification AAA locale pour une ou plusieurs des méthodes de gestion de l'interface de ligne de commande (SSH, Telnet, console série). Les connexions à ASDM ne sont pas enregistrées dans l'historique.

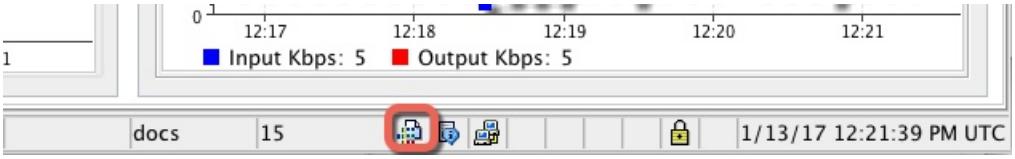
Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Login History (Historique de connexion)**.

Étape 2 Cochez la case **Configure login history reporting for administrators** (Configurer les rapports d'historique de connexion pour les administrateurs). Cette fonction est activée par défaut.

Étape 3 Définissez la **durée** entre 1 et 365 jours. La valeur par défaut est 90.

Étape 4 Pour afficher l'historique de connexion, à partir de n'importe quel écran ASDM, vous pouvez cliquer sur l'icône **Login History** (Historique de connexion) dans la barre **Status** (État) inférieure :



L'historique de connexion de tous les utilisateurs s'affiche dans une boîte de dialogue.

Configurer la traçabilité de l'accès de gestion

Vous pouvez envoyer des messages de traçabilité au serveur de comptabilité TACACS+ lorsque vous saisissez une commande autre que les commandes **show** au niveau de l'interface de ligne de commande. Vous pouvez configurer la comptabilisation lorsque les utilisateurs se connectent, lorsqu'ils saisissent la commande **enable** ou lorsqu'ils émettent des commandes.

Pour la traçabilité des commandes, vous pouvez uniquement utiliser des serveurs TACACS+.

Pour configurer l'accès de gestion et activer la traçabilité des commandes, procédez comme suit :

Procédure

Étape 1 Pour activer la comptabilisation des utilisateurs lorsqu'ils saisissent la commande **enable**, procédez comme suit :

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Accounting (Traçabilité)**, puis cochez la case **Require accounting to allow accounting of user activity (Exiger la traçabilité pour permettre la comptabilisation de l'activité de l'utilisateur)** > **Enable (Activer)**.

b) Choisissez un nom de groupe de serveurs RADIUS ou TACACS+.

Étape 2 Pour activer la comptabilisation des utilisateurs lorsqu'ils accèdent à l'ASA à l'aide de Telnet, de SSH ou de la console de série, procédez comme suit :

a) Cochez les cases **Serial** (Série), **SSH** et/ou **Telnet** dans la zone **Require accounting for the following types of connections** (Exiger la traçabilité pour les types de connexions suivants).

b) Choisissez un nom de groupe de serveurs RADIUS ou TACACS+ pour chaque type de connexion.

Étape 3 Pour configurer la traçabilité des commandes, procédez comme suit :

a) Cochez la case **Enable** (Activer) dans la zone **Require accounting for the following types of connections** (Exiger la traçabilité pour les types de connexions suivants).

b) Choisissez un nom de groupe de serveurs TACACS+. RADIUS n'est pas pris en charge.

Vous pouvez envoyer des messages de traçabilité au serveur de comptabilité TACACS+ lorsque vous saisissez une commande autre que les commandes **show** au niveau de l'interface de ligne de commande.

c) Si vous personnalisez le niveau de privilège des commandes à l'aide de la boîte de dialogue **Command Privilege Setup** (Configuration des privilèges de commande), vous pouvez limiter les commandes pour lesquelles l'ASA est responsable en précisant un niveau de privilège minimum dans la liste déroulante **Privilege level** (Niveau de privilège). L'ASA ne prend pas en compte les commandes dont le niveau de privilège est inférieur.

Étape 4 Cliquez sur **Apply** (Appliquer).

Les paramètres de comptabilisation sont affectés et les modifications sont enregistrées dans la configuration d'exécution.

Récupérer d'un verrouillage

Dans certaines circonstances, lorsque vous activez l'autorisation de commande ou l'authentification de l'interface de ligne de commande, vous pouvez être verrouillé hors de l'interface de ligne de commande de l'ASA. Vous pouvez généralement récupérer l'accès en redémarrant l'ASA. Cependant, si vous avez déjà enregistré votre configuration, vous pourriez être verrouillé.

Le tableau suivant répertorie les conditions de verrouillage courantes et la façon dont vous pouvez y remédier.

Tableau 57 : Scénarios de verrouillage de l'authentification de l'interface de ligne de commande et de l'autorisation de commande

Fonctionnalités	Condition de verrouillage	Description	Solution de contournement : mode unique	Solution de contournement : mode multiple
Authentification de l'interface de ligne de commande locale	Aucun utilisateur n'a été configuré dans la base de données locale.	Si vous n'avez aucun utilisateur dans la base de données locale, vous ne pouvez pas vous connecter ni ajouter d'utilisateurs.	Connectez-vous et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et ajouter un utilisateur.
Autorisation de commande TACACS+ Authentification de l'interface de ligne de commande TACACS+ Authentification de l'interface de ligne de commande RADIUS	Le serveur est en panne ou inaccessible et vous n'avez pas configuré la méthode de secours.	Si le serveur est inaccessible, vous ne pouvez pas vous connecter ni saisir de commandes.	**1.** Connectez-vous et réinitialisez les mots de passe et les commandes AAA. **2.** Configurez la base de données locale comme méthode de secours afin de ne pas être verrouillé lorsque le serveur est en panne.	**1.** Si le serveur est inaccessible en raison d'une configuration de réseau incorrecte sur l'ASA, connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et reconfigurer vos paramètres réseau. **2.** Configurez la base de données locale comme méthode de secours afin de ne pas être verrouillé lorsque le serveur est en panne.
Autorisation de commande TACACS+	Vous êtes connecté en tant qu'utilisateur sans privilèges suffisants ou en tant qu'utilisateur qui n'existe pas.	Vous activez l'autorisation de commande, mais vous constatez ensuite que l'utilisateur ne peut plus saisir de commandes.	Corrigez le compte d'utilisateur du serveur TACACS+. Si vous n'avez pas accès au serveur TACACS+ et que vous devez configurer l'ASA immédiatement, connectez-vous à la partition de maintenance et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et terminer les modifications de configuration. Vous pouvez également désactiver l'autorisation de commande jusqu'à ce que vous corrigiez la configuration TACACS+.
Autorisation de commande locale	Vous êtes connecté en tant qu'utilisateur sans privilèges suffisants.	Vous activez l'autorisation de commande, mais vous constatez ensuite que l'utilisateur ne peut plus saisir de commandes.	Connectez-vous et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et changer le niveau d'utilisateur.

Accès au moniteur

- **Monitoring (Supervision)** > **Properties (Propriétés)** > **Device Access (Accès au périphérique)** > **ASDM/HTTPS/Telnet/SSH Sessions (Sessions ASDM/HTTPS/Telnet/SSH)**

  Le volet supérieur répertorie les types de connexion, les ID de session et les adresses IP des utilisateurs connectés par le biais des sessions ASDM, HTTPS et Telnet. Pour déconnecter une session en particulier, cliquez sur **Disconnect** (Déconnecter).

  Le volet inférieur répertorie les clients, les noms d'utilisateur, les états de connexion, les versions logicielles, les types de chiffrement entrants, les types de chiffrement sortants, les HMAC entrants, les HMAC sortants, les ID de session SSH, les données de renouvellement restantes, le temps de renouvellement restant, les renouvellements basés sur les données, les renouvellements basés sur le temps et l'heure de la dernière reconnexion. Pour déconnecter une session en particulier, cliquez sur **Disconnect** (Déconnecter).

- **Monitoring (Supervision)** > **Properties (Propriétés)** > **Device Access (Accès au périphérique)** > **Authenticated Users (Utilisateurs authentifiés)**

  Ce volet répertorie les noms d'utilisateur, les adresses IP, les listes de contrôle d'accès dynamique, les délais d'inactivité (le cas échéant) et les délais absolus des utilisateurs qui ont été authentifiés par les serveurs AAA.

- **Monitoring (Supervision)** > **Properties (Propriétés)** > **Device Access (Accès au périphérique)** > **AAA Locked Out Users (Utilisateurs AAA verrouillés)**

  Ce volet répertorie les noms d'utilisateur des utilisateurs locaux AAA verrouillés, le nombre de tentatives d'authentification en échec et les heures auxquelles les utilisateurs ont été verrouillés. Pour effacer un utilisateur spécifique qui a été verrouillé, cliquez sur **Clear Selected Lockout** (Effacer le verrouillage sélectionné). Pour effacer tous les utilisateurs qui ont été verrouillés, cliquez sur **Clear All Lockouts** (Effacer tous les verrouillages).

- **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

Historique de l'accès de gestion

Tableau 58 : Historique de l'accès de gestion

Nom de la caractéristique	Versions de plateforme	Description
Pile CiscoSSH maintenant par défaut	9.19(1)	La pile Cisco SSH est maintenant utilisée par défaut. Écrans Nouveaux ou modifiés : • Mode de contexte unique : **Configuration** > **Device Management (Gestion des appareils)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** • Mode de contexte multiple : **Configuration** > **Device Management (Gestion des appareils)** > **SSH Stack (Pile SSH)**

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de l'interface de boucle avec retour pour SSH et Telnet	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour les fonctionnalités suivantes : • SSH • Telnet Commandes nouvelles/modifiées : **interface loopback**, **ssh**, **telnet** Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add Loopback Interface (ajouter une interface de bouclage)**. La prise en charge d'ASDM a été ajoutée dans la version 7.19.
Pile CiscoSSH	9.17(1)	L'ASA utilise une pile SSH propriétaire pour les connexions SSH. Vous pouvez maintenant choisir d'utiliser à la place la pile CiscoSSH, qui est basée sur OpenSSH. La pile par défaut continue d'être la pile ASA. Cisco SSH prend en charge : • Conformité FIPS • Mises à jour régulières, y compris les mises à jour de Cisco et de la communauté de code source libre. Notez que la pile CiscoSSH ne prend pas en charge : • SSH vers une interface différente sur VPN (accès de gestion) • Paire de clés EdDSA • Paire de clés RSA en mode FIPS Si vous avez besoin de ces fonctionnalités, vous devez continuer à utiliser la pile SSH ASA. Il y a une petite modification de la fonctionnalité SCP avec la pile CiscoSSH : pour utiliser la commande **copy** de l'ASA pour copier un fichier vers ou à partir d'un serveur SCP, vous devez activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP. Écrans Nouveaux ou modifiés : • Mode de contexte unique : **Configuration** > **Device Management (Gestion des appareils)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** • Mode de contexte multiple : **Configuration** > **Device Management (Gestion des appareils)** > **SSH Stack (Pile SSH)**

Nom de la caractéristique	Versions de plateforme	Description
Modifications du verrouillage de l'utilisateur local	9.17(1)	L'ASA peut verrouiller les utilisateurs locaux après un nombre configurable de tentatives de connexion échouées. Cette fonctionnalité ne s'applique pas aux utilisateurs ayant le niveau de privilège 15. De plus, un utilisateur serait verrouillé indéfiniment jusqu'à ce qu'un administrateur déverrouille son compte. Désormais, les utilisateurs seront déverrouillés après 10 minutes, à moins qu'un administrateur n'utilise la commande **clear aaa local user lockout** avant. Les utilisateurs ayant le niveau de privilège 15 sont également concernés par le paramètre de verrouillage. Commandes nouvelles ou modifiées : **aaa local authentication attempts max-fail** , **show aaa local user**
Invite de modification du mot de passe SSH et Telnet	9.17(1)	La première fois qu'un utilisateur local se connecte à l'ASA à l'aide de SSH ou de Telnet, il est invité à changer de mot de passe. Il sera également invité à se connecter pour la première fois après qu'un administrateur aura modifié son mot de passe. Si l'ASA se recharge, les utilisateurs ne seront pas invités, même s'il s'agit de leur première connexion. Notez que tout service qui utilise la base de données des utilisateurs locale, comme VPN, devra également utiliser le nouveau mot de passe s'il a été modifié lors d'une connexion SSH ou Telnet. Commandes nouvelles ou modifiées : **show aaa local user**

Nom de la caractéristique	Versions de plateforme	Description
Améliorations de la sécurité SSH	9.16(1)	SSH prend désormais en charge les améliorations de sécurité suivantes : • Format de clé d'hôte : **crypto key generate** {**eddsa** | **ecdsa**}. En plus de RSA, nous avons ajouté la prise en charge des clés d'hôte EdDSA et ECDSA. L'ASA essaie d'utiliser les clés dans l'ordre suivant, si elles existent : EdDSA, ECDSAA, puis RSA. Si vous configurez explicitement l'ASA pour utiliser la clé RSA avec la commande **ssh key-exchange hostkey rsa**, vous devez générer une clé de 2 048 bits ou plus. Pour des raisons de compatibilité avec les mises à niveau, l'ASA utilisera des clés hôtes RSA de plus petite taille uniquement lorsque le paramètre par défaut de la clé hôte est utilisé. La prise en charge de RSA sera supprimée dans une version ultérieure. • Algorithmes d'échange de clés : **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • Algorithmes de chiffrement : **ssh cipher encryption chacha20-poly1305@openssh.com** • La version 1 de SSH n'est plus prise en charge. La commande **ssh version** est supprimée. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** • **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)** • **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffrement SSH)**
Accès de gestion pour SNMP	9.14(2)	Lors de la configuration de l'accès de gestion sur un tunnel VPN, incluez l'adresse IP de l'interface externe dans la liste d'accès de la carte cryptographique dans le cadre de la configuration du VPN pour sécuriser l'interrogation SNMP sur un VPN de site à site.

Nom de la caractéristique	Versions de plateforme	Description
Paramètre de délai d'inactivité HTTPS	9.14(1)	Vous pouvez maintenant définir le délai d'inactivité pour toutes les connexions HTTPS à l'ASA, y compris ASDM, WebVPN et d'autres clients. Auparavant, avec la commande **http server idle-timeout**, vous pouviez uniquement définir le délai d'inactivité d'ASDM. Si vous définissez les deux délais, la nouvelle commande prévaut. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** > **HTTP Settings (Paramètres HTTP)** > **case Connection Idle Timeout (Délai d'inactivité de la connexion)**.
Le chiffrement SSH est désormais répertorié (de la sécurité la plus haute à la plus basse) pour les listes prédéfinies	9.13(1)	Le chiffrement SSH est désormais répertorié (de la sécurité la plus haute à la sécurité la plus basse) pour les listes prédéfinies (comme moyen ou élevé). Dans les versions précédentes, il était répertorié du niveau le plus bas au plus élevé, ce qui signifie qu'un chiffrement à faible sécurité serait proposé avant un chiffrement à sécurité élevée. Écrans Nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffrement SSH)**
La définition du mode d'échange de clés SSH est limitée au contexte d'administration	9.12(2)	Vous devez définir l'échange de clés SSH dans le contexte d'administration; ce paramètre est hérité par tous les autres contextes. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** > **SSH Settings (Paramètres SSH)** > **DH Key Exchange (Échange de clés DH)**
Le changement de mot de passe **enable** est maintenant requis lors de la connexion	9.12(1)	Le mot de passe par défaut **enable** est vide. Lorsque vous essayez d'accéder en mode d'exécution privilégié sur l'ASA, vous devez désormais modifier le mot de passe pour une valeur de 3 caractères ou plus. Vous ne pouvez pas le garder vide. La commande **no enable password** n'est plus prise en charge. Au niveau de l'interface de ligne de commande, vous pouvez accéder au mode d'exécution privilégié à l'aide des commandes **enable**, **login** (avec un utilisateur de niveau de privilège 2+), ou d'une session SSH ou Telnet lorsque vous activez **aaa authorization exec auto-enable**. Toutes ces méthodes nécessitent que vous définissiez le mot de passe d'activation. Cette exigence de changement de mot de passe n'est pas appliquée pour les connexions ASDM. Dans ASDM, par défaut, vous pouvez vous connecter sans nom d'utilisateur et avec le mot de passe **enable**. Aucun écran modifié.

Nom de la caractéristique	Versions de plateforme	Description
Limitation configurable des sessions d'administration	9.12(1)	Vous pouvez configurer le nombre maximum de sessions administratives agrégées, par utilisateur et par protocole. Auparavant, vous pouviez configurer uniquement le nombre agrégé de sessions. Cette fonctionnalité n'influe pas sur les sessions de console. Notez qu'en mode de contexte multiple, vous ne pouvez pas configurer le nombre de sessions HTTPS, où le maximum est fixé à 5 sessions. La commande **quota management-session** n'est également plus acceptée dans la configuration système et est plutôt disponible dans la configuration du contexte. Le nombre maximum de sessions agrégées est désormais de 15; si vous avez configuré 0 (illimité) ou 16+, lors de la mise à niveau, la valeur passe à 15. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Management Session Quota (Quota de sessions de gestion)**
Notifications pour les modifications du niveau de privilège d'administration	9.12(1)	Lorsque vous vous authentifiez pour activer l'accès (**aaa authentication enable console**) ou autorisez directement l'accès EXEC privilégié (**aaa authorization exec auto-enable**), l'ASA informe désormais les utilisateurs si le niveau d'accès qui leur a été attribué a changé depuis leur dernière connexion. Écrans Nouveaux ou modifiés : Barre **Status (État)** > icône **Login History (Historique de connexion)**
Sécurité SSH renforcée	9.12(1)	Consultez les améliorations de sécurité SSH suivantes : • Prise en charge de l'échange de clés SHA256, groupe Diffie-Hellman 14. Ce paramètre est désormais la valeur par défaut. L'ancienne valeur par défaut était le groupe 1 SHA1. • Prise en charge du chiffrement d'intégrité HMAC-SHA256. La valeur par défaut est désormais l'ensemble de chiffrements à haute sécurité (hmac-sha2-256 uniquement). L'ancienne valeur par défaut était l'ensemble moyen. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** • **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffrement SSH)**

Nom de la caractéristique	Versions de plateforme	Description
Autoriser les clients HTTPS non basés sur le navigateur à accéder à l'ASA	9.12(1)	Vous pouvez autoriser les clients HTTPS non basés sur le navigateur à accéder aux services HTTPS sur l'ASA. Par défaut, ASDM, CSM et l'API REST sont autorisés. Écrans nouveaux ou modifiés. **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **HTTP Non-Browser Client Support (Prise en charge des clients HTTP non basés sur le navigateur)**
La paire de clés RSA prend en charge les clés de 3 072 bits	9.9(2)	Vous pouvez maintenant définir la taille du module à 3 072. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)**
Accès de gestion du VPN sur les interfaces virtuelles pontées (BVI)	9.9(2)	Vous pouvez maintenant activer des services de gestion, tels que **telnet**, **http** et **ssh**, sur une BVI si le paramètre **management-access** du VPN a été activé sur cette BVI. Pour l'accès de gestion non VPN, vous devez continuer à configurer ces services sur les interfaces membres du groupe de ponts. Commandes nouvelles ou modifiées : **https**, **telnet**, **ssh**, **management-access**
La version 1 de SSH est obsolète	9.9(1)	La version 1 de SSH est obsolète et sera supprimée dans une version ultérieure. Le paramètre par défaut est passé de SSH v1 et v2 à SSH v2. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH**

Nom de la caractéristique	Versions de plateforme	Description
Authentification distincte pour les utilisateurs disposant d'une authentification par clé publique SSH et les utilisateurs disposant de mots de passe	9.6(3)/9.8(1)	Dans les versions antérieures à 9.6(2), vous pouviez activer l'authentification par clé publique SSH (**ssh authentication**) sans activer explicitement l'authentification SSH AAA avec la base de données des utilisateurs locale (**aaa authentication ssh console LOCAL**). Dans 9.6(2), l'ASA vous a demandé d'activer explicitement l'authentification SSH AAA. Dans cette version, vous n'avez plus à activer explicitement l'authentification SSH AAA; lorsque vous configurez la commande **ssh authentication** pour un utilisateur, l'authentification locale est activée par défaut pour les utilisateurs avec ce type d'authentification. De plus, lorsque vous configurez explicitement l'authentification SSH AAA, cette configuration s'applique uniquement aux noms d'utilisateur avec *mots de passe*, et vous pouvez utiliser n'importe quel type de serveur AAA (**aaa authentication ssh console radius_1**, par exemple). Par exemple, certains utilisateurs peuvent utiliser l'authentification par clé publique à l'aide de la base de données locale et d'autres utilisateurs peuvent utiliser des mots de passe avec RADIUS. Nous n'avons pas modifié d'écrans.
Historique de connexion	9.8(1)	Par défaut, l'historique de connexion est enregistré pendant 90 jours. Vous pouvez désactiver cette fonctionnalité ou modifier la durée, jusqu'à 365 jours. Cette fonctionnalité s'applique uniquement aux noms d'utilisateur dans la base de données locale lorsque vous activez l'authentification AAA locale pour une ou plusieurs des méthodes de gestion (SSH, ASDM, Telnet, etc.). Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Login History (Historique de connexion)**
Application de la politique de mot de passe pour interdire la réutilisation des mots de passe et l'utilisation d'un mot de passe correspondant à un nom d'utilisateur	9.8(1)	Vous pouvez désormais interdire la réutilisation des mots de passe précédents pour un maximum de 7 générations, et vous pouvez également interdire l'utilisation d'un mot de passe correspondant à un nom d'utilisateur. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Password Policy (Politique de mot de passe)**
Mode du serveur SSL ASA correspondant à ASDM	9.6(2)	Pour un utilisateur ASDM qui s'authentifie avec un certificat, vous pouvez désormais exiger que le certificat corresponde à une carte de certificat. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH**

Nom de la caractéristique	Versions de plateforme	Description
Améliorations de l'authentification par clé publique SSH	9.6(2)	Dans les versions antérieures, vous pouviez activer l'authentification par clé publique SSH sans activer également l'authentification SSH AAA avec la base de données d'utilisateurs locale . La configuration est désormais modifiée de manière à ce que vous deviez explicitement activer l'authentification SSH AAA. Pour empêcher les utilisateurs d'utiliser un mot de passe au lieu de la clé privée, vous pouvez désormais créer un nom d'utilisateur sans mot de passe défini. Nous avons modifié les écrans suivants : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)**
Autorisation de gestion ASDM	9.4(1)	Vous pouvez désormais configurer l'autorisation de gestion séparément pour l'accès HTTP par rapport à l'accès Telnet et SSH. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Autorisation)**
Nom d'utilisateur ASDM dans la configuration du certificat	9.4(1)	Lorsque vous activez l'authentification par certificat ASDM, vous pouvez configurer la façon dont ASDM extrait le nom d'utilisateur du certificat; vous pouvez également activer le préremplissage du nom d'utilisateur à l'invite de connexion. Nous avons introduit l'écran suivant : **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > HTTP Certificate Rule (Règle de certificat HTTP).**
Authentification par mot de passe à usage unique améliorée	9.2(1)	Les administrateurs qui disposent de privilèges d'autorisation suffisants peuvent passer en mode d'exécution privilégié en saisissant une seule fois leurs informations d'authentification. L'option **auto-enable** a été ajoutée à la commande **aaa authorization exec**. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Authorization (Autorisation).
Prise en charge de la redirection HTTP pour IPV6	9.1(7)/9.6(1)	Lorsque vous activez la redirection HTTP vers HTTPS pour l'accès ASDM ou le SSL VPN sans client, vous pouvez désormais rediriger le trafic envoyé par vers l'adresse IPv6. Nous avons ajouté des fonctionnalités à l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **HTTP Redirect (Redirection HTTP)**

Nom de la caractéristique	Versions de plateforme	Description
Chiffrement SSH et d'intégrité configurables	9.1(7.4), 9.5(3), 9.6(1)	Les utilisateurs peuvent sélectionner des modes de chiffrement lors de la gestion du chiffrement SSH et peuvent configurer le HMAC et le chiffrement pour divers algorithmes d'échange de clés. Vous souhaiterez peut-être modifier les chiffres pour qu'ils soient plus ou moins stricts, selon votre application. Notez que la performance de la copie sécurisée dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier les chiffres proposés, utilisez **ssh cipher encryption custom aes128-cbc**, par exemple. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffres SSH)**
Chiffrement AES-CTR pour SSH	9.1(2)	La mise en œuvre du serveur SSH dans l'ASA prend désormais en charge le chiffrement en mode AES-CTR.
Intervalle de renouvellement SSH amélioré	9.1(2)	Une connexion SSH est renouvelée après 60 minutes de connexion ou 1 Go de trafic de données. .
Pour l'ASASM en mode de contexte multiple, prenez en charge l'authentification Telnet et de la console virtuelle à partir du commutateur.	8.5(1)	Bien que la connexion à l'ASASM à partir du commutateur en mode de contexte multiple se connecte à l'espace d'exécution du système, vous pouvez configurer l'authentification dans le contexte d'administration pour régir ces connexions.
Prise en charge de la politique de mot de passe administrateur lors de l'utilisation de la base de données locale	8.4(4.1), 9.1(2)	Lorsque vous configurez l'authentification pour l'accès à l'interface de ligne de commande ou à ASDM à l'aide de la base de données locale, vous pouvez configurer une politique de mot de passe qui oblige un utilisateur à changer de mot de passe après une durée spécifiée et qui exige également des normes de mot de passe tel qu'une longueur minimum et le nombre minimum de modifications de caractères. Nous avons introduit l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > Password Policy (Politique de mot de passe).

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de l'authentification par clé publique SSH	8.4(4.1), 9.1(2)	Vous pouvez activer l'authentification par clé publique pour les connexions SSH à l'ASA par utilisateur. Vous pouvez spécifier une clé formatée de fichier de clé publique (PKF) ou une clé Base64. La clé PKF peut comporter jusqu'à 4 096 bits. Utilisez le format PKF pour les clés qui sont trop grandes pour la prise en charge ASA du format Base64 (jusqu'à 2 048 bits). Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs) > Edit User Account (Modifier le compte d'utilisateur) > Public Key Authentication (Authentification par clé publique) Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs) > Edit User Account (Modifier le compte d'utilisateur) > Public Key Using PKF (Clé publique utilisant PKF). *Le format de clé PKF est uniquement pris en charge dans la version 9.1(2) et les versions ultérieures.*
Prise en charge du groupe Diffie-Hellman 14 pour l'échange de clés SSH	8.4(4.1), 9.1(2)	La prise en charge du groupe Diffie-Hellman 14 pour l'échange de clés SSH a été ajoutée. Auparavant, seul le groupe 1 était pris en charge. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > ASDM/HTTPS/Telnet/SSH.
Prise en charge d'un nombre maximum de sessions de gestion	8.4(4.1), 9.1(2)	Vous pouvez définir le nombre maximum de sessions ASDM, SSH et Telnet simultanées. Nous avons introduit l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > Management Session Quota (Quota de sessions de gestion).
Sécurité SSH améliorée; le nom d'utilisateur SSH par défaut n'est plus pris en charge.	8.4(2)	À partir de la version 8.4(2), vous ne pouvez plus vous connecter à l'ASA à l'aide de SSH avec le nom d'utilisateur pix ou asa et le mot de passe de connexion. Pour utiliser SSH, vous devez configurer l'authentification AAA à l'aide de la commande **aaa authentication ssh console LOCAL** (interface de ligne de commande) ou Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Authentication (ASDM) (Authentification (ASDM)); puis définissez un utilisateur local en saisissant la commande **username** (interface de ligne de commande) ou en sélectionnant Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (ASDM) (Comptes d'utilisateurs (ASDM)). Si vous souhaitez utiliser un serveur AAA pour l'authentification au lieu de la base de données locale, nous vous conseillons de configurer également l'authentification locale comme méthode de sauvegarde.

Nom de la caractéristique	Versions de plateforme	Description
Accès de gestion	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > ASDM/HTTPS/Telnet/SSH Configuration (Configuration ASDM/HTTPS/Telnet/SSH) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > Command Line (CLI) Ligne de commande (Interface de ligne de commande) > Banner Configuration (Configuration de la bannière) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > CLI Prompt Configuration (Configuration de l'invite de l'interface de ligne de commande) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > ICMP Configuration (Configuration ICMP) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > FTP Client Configuration (Configuration du client FTP) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > Secure Copy (SCP) Server Configuration (Configuration du serveur de copie sécurisée) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > Mount-Points Configuration (Configuration des points de montage) > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Authentication Configuration (Configuration de l'authentification) > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Authorization Configuration (Configuration de l'autorisation) > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Accounting (Comptabilisation).



CHAPITRE 45

Logiciels et configurations

Ce chapitre décrit comment gérer le logiciel et les configurations ASA.

- Mettre à niveau le logiciel, à la page 1185
- Charger une image à l'aide de ROMMON (ISA 3000), à la page 1185
- Mettre à niveau l'image ROMMON : ISA 3000, à la page 1187
- Rétrograder votre logiciel, à la page 1188
- Gérer les fichiers, à la page 1193
- Définir l'image ASA, ASDM et la configuration de démarrage, à la page 1201
- Sauvegarde et restauration de configurations ou d'autres fichiers, à la page 1203
- Programmer un redémarrage du système, à la page 1210
- Échange à chaud d'un SSD sur Cisco Secure Firewall , à la page 1211
- Historique des logiciels et des configurations, à la page 1213

Mettre à niveau le logiciel

Consultez le Guide de mise à niveau de Cisco ASA pour accéder aux procédures de mise à niveau complètes.

Charger une image à l'aide de ROMMON (ISA 3000)

Pour charger une image logicielle sur un ASA en mode ROMMON à l'aide de TFTP, procédez comme suit.

Procédure

Étape 1 Connectez-vous au port de la console de l'ASA en suivant les instructions de Accéder à la console de l'ISA 3000, à la page 17.

Étape 2 Mettez l'ASA hors tension, puis rallumez-le.

Étape 3 Pendant le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à passer en mode ROMMON.

Étape 4 En mode ROMMON, définissez les paramètres d'interface avec l'ASA, notamment l'adresse IP, l'adresse du serveur TFTP, l'adresse de la passerelle, le fichier d'image logicielle et le port, comme suit :

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
```

```
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

Remarque Assurez-vous que la connexion au réseau est déjà établie.

Sur les plateformes ASA 5506-X, ASA 5508-X, ASA 5516-X et ISA 3000, la commande **interface** ne fonctionne pas, ce qui oblige à utiliser l'interface Management 1/1 pour la récupération TFTP.

Étape 5 Validez les paramètres :

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

Étape 6 Envoyez un message Ping au serveur TFTP :

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

Étape 7 Enregistrez les paramètres réseau pour une utilisation ultérieure :

```
rommon #8> sync
Updating NVRAM Parameters...
```

Étape 8 Chargez l'image logicielle :

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes
```

```
Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

Une fois l'image logicielle chargée, l'ASA quitte automatiquement le mode ROMMON.

Étape 9 Le démarrage de l'ASA en mode ROMMON ne permet pas de conserver l'image du système après un rechargement. Vous devez donc télécharger l'image dans la mémoire flash. Consultez le Guide de mise à niveau de Cisco ASA pour accéder aux procédures de mise à niveau complètes.

Mettre à niveau l'image ROMMON : ISA 3000

Pour les ISA 3000, procédez comme suit afin de mettre à niveau l'image ROMMON. Pour les modèles ASA, vous devez avoir installé la version 1.1.8 ou toute version ultérieure de ROMMON sur votre système. Nous vous recommandons d'effectuer la mise à niveau vers la dernière version.

Seule une mise à niveau vers une nouvelle version est possible; la rétrogradation n'est pas prise en charge.

Mise en garde La ISA 3000 prend deux fois plus de temps que pour les versions précédentes (environ 15 minutes). **N'éteignez pas** l'appareil pendant la mise à niveau. Si la mise à niveau prend plus de 30 minutes ou si elle échoue, contactez l'assistance technique de Cisco. **N'éteignez pas** l'appareil et ne le réinitialisez pas.

Avant de commencer

Procurez-vous la nouvelle image ROMMON sur Cisco.com et enregistrez-la sur un serveur pour ensuite la copier sur l'ASA. L'ASA prend en charge les serveurs FTP, TFTP, SCP, HTTP(S) et SMB. Téléchargez l'image de :

- ISA 3000 : https://software.cisco.com/download/home/286288493/type

Procédure

Étape 1 Copiez l'image ROMMON sur la mémoire flash de l'ASA. Cette procédure illustre la commande « copy FTP ». Entrez **copy ?** pour la syntaxe appropriée pour les autres types de serveurs.

copy ftp://[*noms d'utilisateur***:***mot de passe***@**]*server_ip*/**asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

Étape 2 Pour connaître la version installée, entrez la commande **show module** et consultez la version du pare-feu (FW) dans la sortie du module 1 du tableau des plages d'adresses MAC :

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
```

```
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

Étape 3 Procédez à la mise à niveau de l'image ROMMON :

upgrade rommon disk0:asa5500-firmware-*XXXX*.SPA

Exemple :

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

Étape 4 Lorsque vous y êtes invité, appuyez sur Confirmer pour recharger l'ASA.

L'ASA met à niveau l'image ROMMON, puis recharge le système d'exploitation.

Rétrograder votre logiciel

Dans de nombreux cas, vous pouvez rétrograder votre logiciel ASA et restaurer une configuration de sauvegarde à partir de la version de logiciel précédemment installée. La méthode de rétrogradation dépend de votre plateforme ASA.

Directives et limites en matière de rétrogradation

Consultez les consignes suivantes avant la rétrogradation :

- **Il n'y a pas de prise en charge officielle de la rétrogradation sans temps d'arrêt pour la mise en grappe**. Cependant la rétrogradation sans temps d'arrêt fonctionnera dans certains cas. Si vous rencontrez des problèmes, vous devez recharger vos unités de grappe, ce qui entraîne un temps d'arrêt.

- **Problème de rétrogradation de la version 9.18 ou ultérieure** : il y a un changement de comportement dans la version 9.18 où la commande **access-group** sera répertoriée avant ses commandes **access-list**. Si vous effectuez une rétrogradation, la commande **access-group** sera rejetée, car elle n'a pas encore chargé les commandes **access-list**. Ce résultat se produit même si vous avez précédemment activé la commande **forward-reference enable**, car cette commande est maintenant supprimée. Avant de procéder à la rétrogradation, assurez-vous de copier toutes les commandes **access-group** manuellement, puis après la rétrogradation, saisissez-les de nouveau.
- **Les tunnels VPN sont répliqués sur l'unité de secours même si cette dernière exécute une version du logiciel qui ne prend pas en charge la suite de chiffrement que le tunnel d'origine a négociée.** Ce scénario se produit lors de la rétrogradation. Dans ce cas, déconnectez votre connexion VPN et reconnectez-vous.

Configuration incompatible supprimée après la rétrogradation

Lorsque vous effectuez une rétrogradation à une ancienne version, les commandes qui ont été introduites dans les versions ultérieures seront supprimées de la configuration. Il n'existe aucun moyen automatisé de vérifier la configuration par rapport à la version cible avant de procéder à la rétrogradation. Vous pouvez découvrir quand de nouvelles commandes ont été ajoutées dans les nouvelles fonctionnalités d'ASA par version.

Vous pouvez afficher les commandes rejetées *après* avoir effectué une rétrogradation en utilisant la commande **show startup-config errors**. Si vous pouvez rétrograder un périphérique de laboratoire, vous pouvez prévisualiser les effets en utilisant cette commande avant de rétrograder un périphérique de production.

Dans certains cas, l'ASA migre automatiquement les commandes vers de nouveaux formulaires lors de la mise à niveau. Ainsi, selon votre version, même si vous n'avez pas configuré manuellement de nouvelles commandes, la rétrogradation peut être influencée par les migrations de configuration. Nous vous recommandons de sauvegarder votre ancienne configuration logicielle afin de pouvoir l'utiliser lors de la rétrogradation. Dans le cas d'une mise à niveau vers la version 8.3, une sauvegarde est automatiquement créée (<old_version>_startup_cfg.sav). Les autres migrations ne créent pas de sauvegardes. Consultez les « Directives et migrations propres à la version » dans le guide de mise à niveau d'ASA pour en savoir plus sur les migrations automatiques des commandes qui pourraient avoir une incidence sur la rétrogradation.

Consultez également les problèmes de rétrogradation connus dans Directives et limites en matière de rétrogradation, à la page 1188.

Par exemple, un ASA utilisant la version 9.8(2) inclut les commandes suivantes :

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
```

Lorsque vous rétrogradez le périphérique à la version 9.0(4), les erreurs suivantes s'afficheront au démarrage :

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
                                       ^
ERROR: % Invalid input detected at '^' marker.

username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                                ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
```

```
                                                ^
ERROR: % Invalid input detected at '^' marker.
```

Dans cet exemple, la prise en charge de **sctp** dans la commande **access-list étendue** a été ajoutée dans la version 9.5(2), la prise en charge de **pbkdf2** dans la commande **username** a été ajoutée dans la version 9.6(1) et la prise en charge de **engineID** dans la commande **snmp-server user** a été ajouté dans la version 9.5(3).

Rétrograder l'appareil ASA

Vous pouvez rétrograder la version du logiciel de l'ASA en définissant la version de l'ASA sur l'ancienne version, en restaurant la configuration de sauvegarde dans la configuration de démarrage, puis en la rechargeant. Cette procédure s'applique aux modèles suivants :

- Firepower 1000
- Secure Firewall 1200
- Firepower de la série 2100
- Secure Firewall 3100
- Secure Firewall 4200

Avant de commencer

Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration. Si vous ne restaurez pas l'ancienne configuration, vous risquez d'avoir des commandes incompatibles représentant des fonctionnalités nouvelles ou modifiées. Toute nouvelle commande sera rejetée lorsque vous chargerez l'ancienne version du logiciel.

Procédure

Étape 1 Chargez l'ancienne version du logiciel ASA en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe. Dans ce cas, précisez l'ancienne version d'ASA au lieu d'une nouvelle version. **Important :** Ne rechargez *pas* encore l'ASA.

Étape 2 Au niveau de l'interface de ligne de commande de l'ASA, copiez la configuration de l'ASA de secours dans la configuration de démarrage. Pour le basculement, effectuez cette étape sur l'unité active. Cette étape réplique la commande sur l'unité de secours.

copy *ancienne_url_de_configuration* **startup-config**

Il est important que vous n'enregistriez pas la configuration en cours dans la configuration de démarrage à l'aide de **write memory**; cette commande remplacera votre configuration de sauvegarde.

Exemple :

```
ciscoasa# copy disk0:/9.13.1_cfg.sav startup-config
```

Étape 3 Rechargez l'ASA.

Interface de ligne de commande ASA

reload

ASDM

Choisissez **Tools (Outils)** > **System Reload (Rechargement du système)**.

Rétrograder le Firepower 2100 en mode plateforme

Vous pouvez rétrograder la version du logiciel de l'ASA en restaurant la configuration de sauvegarde à la configuration de lancement, en réglant la version de l'ASA à l'ancienne version, puis en rechargeant l'unité.

Avant de commencer

Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration. Si vous ne restaurez pas l'ancienne configuration, vous risquez d'avoir des commandes incompatibles représentant des fonctionnalités nouvelles ou modifiées. Toute nouvelle commande sera rejetée lorsque vous chargerez l'ancienne version du logiciel.

Procédure

Étape 1 Au niveau de l'interface de ligne de commande de l'ASA, copiez la configuration de l'ASA de secours dans la configuration de démarrage. Pour le basculement, effectuez cette étape sur l'unité active. Cette étape réplique la commande sur l'unité de secours.

copy *ancienne_url_de_configuration* **startup-config**

Il est important que vous n'enregistriez pas la configuration en cours dans la configuration de démarrage à l'aide de **write memory**; cette commande remplacera votre configuration de sauvegarde.

Exemple :

```
ciscoasa# copy disk0:/9.12.4_cfg.sav startup-config
```

Étape 2 Dans FXOS, utilisez le Firewall Chassis Manager ou l'interface de ligne de commande de FXOS pour utiliser l'ancienne version du logiciel ASA en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe. Dans ce cas, précisez l'ancienne version d'ASA au lieu d'une nouvelle version.

Rétrograder le Firepower 4100/9300

Vous pouvez rétrograder la version du logiciel de l'ASA en restaurant la configuration de sauvegarde à la configuration de lancement, en réglant la version de l'ASA à l'ancienne version, puis en rechargeant l'unité.

Avant de commencer

- Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration. Si vous ne restaurez pas l'ancienne configuration, vous risquez d'avoir des commandes incompatibles représentant des fonctionnalités nouvelles ou modifiées. Toute nouvelle commande sera rejetée lorsque vous chargerez l'ancienne version du logiciel.

- Assurez-vous que l'ancienne version de l'ASA est compatible avec la version de FXOS actuelle. Si ce n'est pas le cas, rétrogradez FXOS en premier lieu avant de restaurer l'ancienne configuration ASA. Assurez-vous que l'instance rétrogradée de FXOS est également compatible avec la version d'ASA actuelle (avant de la rétrograder). Si vous ne parvenez pas à assurer la compatibilité, nous vous conseillons de ne pas procéder à une rétrogradation.

Procédure

Étape 1 Au niveau de l'interface de ligne de commande de l'ASA, copiez la configuration de l'ASA de secours dans la configuration de démarrage. Pour le basculement ou la mise en grappe, effectuez cette étape sur l'unité active/de contrôle. Cette étape réplique la commande sur les unités de secours/de données.

copy *ancienne_url_de_configuration* **startup-config**

Il est important que vous n'enregistriez pas la configuration en cours dans la configuration de démarrage à l'aide de **write memory**; cette commande remplacera votre configuration de sauvegarde.

Exemple :

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

Étape 2 Dans FXOS, utilisez le Firewall Chassis Manager ou l'interface de ligne de commande de FXOS pour utiliser l'ancienne version du logiciel ASA en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe. Dans ce cas, précisez l'ancienne version d'ASA au lieu d'une nouvelle version.

Étape 3 Si vous rétrogradez également FXOS, utilisez le Firewall Chassis Manager ou l'interface de ligne de commande de FXOS pour définir l'ancienne version du logiciel FXOS pour qu'elle soit la version actuelle en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe.

Rétrograder l'ISA 3000

La fonctionnalité de rétrogradation fournit un raccourci pour effectuer les fonctions suivantes sur les modèles ISA 3000 :

- Effacement de la configuration de l'image de démarrage (**clear configure boot**).
- Définition de l'image de démarrage comme étant l'ancienne image (**boot system**).
- (Facultatif) Entrée d'une nouvelle clé d'activation (**activation-key**).
- Enregistrement de la configuration en cours pour le démarrage (**write memory**). Cette opération définit la variable d'environnement BOOT sur l'ancienne image, de sorte que lorsque vous rechargez, l'ancienne image est chargée.
- Copie de l'ancienne sauvegarde de configuration dans la configuration de démarrage (**copy** *ancienne_url_de_configuration* **startup-config**).
- Rechargement (**reload**).

Avant de commencer

- Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration.

Procédure

Étape 1 choisissez **Outils** > **Rétrograder le logiciel**.

La boîte de dialogue Rétrograder le logiciel s'affiche.

Étape 2 Pour l'**image ASA**, cliquez sur **Sélectionner un fichier d'image**.

La boîte de dialogue **Parcourir les emplacements des fichiers** s'affiche.

Étape 3 Cliquez sur l'un des boutons radio suivants :

- **Serveur distant** : choisissez ftp, smb ou http dans la liste déroulante, puis saisissez le chemin d'accès à l'ancien fichier image.
- **Système de fichiers flash** : cliquez sur **Parcourir la mémoire flash** pour choisir l'ancien fichier image sur le système de fichiers flash local.

Étape 4 Pour la **configuration**, cliquez sur **Parcourir la mémoire flash** pour choisir le fichier de configuration de pré-migration.

Étape 5 (Facultatif) Dans le champ **Clé d'activation**, saisissez l'ancienne clé d'activation si vous devez rétablir une clé d'activation antérieure à la version 8.3.

Étape 6 Cliquez sur **Rétrograder**.

Gérer les fichiers

ASDM fournit un ensemble d'outils de gestion de fichiers pour vous aider à effectuer des tâches de gestion de fichiers de base. L'outil de gestion de fichiers vous permet d'afficher, de déplacer, de copier et de supprimer des fichiers stockés dans la mémoire flash, de transférer des fichiers et de gérer des fichiers sur des périphériques de stockage distants (points de montage).

Remarque En mode de contexte multiple, cet outil est uniquement disponible dans le contexte de sécurité du système.

Configurer l'accès au fichier

L'ASA peut utiliser un client FTP, un client de copie sécurisée ou un client TFTP. Vous pouvez également configurer l'ASA en tant que serveur de copie sécurisée afin de pouvoir utiliser un client de copie sécurisée sur votre ordinateur.

Configurer le mode client FTP

L'ASA peut utiliser FTP pour charger ou télécharger des fichiers image ou des fichiers de configuration vers ou depuis un serveur FTP. En mode FTP passif, le client initie à la fois la connexion de contrôle et la connexion de données. Le serveur, qui est le destinataire de la connexion de données en mode passif, répond par le numéro de port sur lequel il écoute pour la connexion spécifique.

Procédure

Étape 1 Dans le volet Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > FTP Client (Client FTP), cochez la case **Specify FTP mode as passive** (Spécifier le mode FTP comme passif).

Étape 2 Cliquez sur **Apply** (Appliquer).

La configuration du client FTP est modifiée et la modification est enregistrée dans la configuration en cours d'exécution.

Configurer l'ASA Secure Copy Client

Vous pouvez configurer les paramètres SCP à l'aide de la commande **copy**.

La performance de SCP dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier le chiffrement proposé, utilisez la commande **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffrement SSH)** ; par exemple, choisissez **Custom** (Personnalisé) et définissez-le sur aes128-cbc.

Avant de commencer

- La licence ASA doit avoir la licence de cryptage renforcé (3DES/AES) pour prendre en charge les connexions SSH version 2.
- Sauf indication contraire, pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, dans le volet Configuration > Device List (Liste des périphériques), double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.
- Pour le serveur SCP, activez SSH sur l'ASA conformément à Configurer l'accès SSH, à la page 1138.

Procédure

Étape 1 Selon votre mode de contexte :

- Pour le mode unique, choisissez **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > Secure Copy (SCP) (Copie sécurisée (SCP))**.

- Pour le mode multiple dans le système, choisissez **Configuration > Device Management (Gestion des périphériques) > Device Administration (Administration des périphériques) > Secure Copy (Copie sécurisée)**

Étape 2 (Facultatif) L'ASA stocke la clé d'hôte SSH pour chaque serveur SCP auquel elle se connecte. Vous pouvez ajouter ou supprimer manuellement des serveurs et leurs clés de la base de données ASA si vous le souhaitez.

Pour ajouter une clé :

a) Cliquez sur **Add** (Ajouter) pour un nouveau serveur ou sélectionnez le serveur dans le tableau des hôtes SSH de confiance, puis cliquez sur **Edit** (Modifier).
b) Pour un nouveau serveur, dans le champ Host (Hôte), saisissez l'adresse IP du serveur.
c) Cochez la case **Add public key for the trusted SSH host** (Ajouter une clé publique pour l'hôte SSH de confiance).
d) Spécifiez l'une des clés suivantes :

- Fingerprint (empreinte) : saisissez la clé déjà hachée; par exemple, une clé que vous avez copiée à partir de la sortie de la commande **show**.
- Key (Clé) : saisissez la clé publique ou la valeur de hachage de l'hôte SSH. La chaîne de clés est la clé publique RSA codée en Base64 de l'homologue distant. Vous pouvez obtenir la valeur de clé publique à partir d'un client SSH ouvert; c'est-à-dire du fichier .ssh/id_rsa.pub. Après avoir soumis la clé publique codée en Base64, cette clé est ensuite hachée au moyen de SHA-256.

Pour supprimer une clé, sélectionnez le serveur dans le tableau des hôtes SSH de confiance, puis cliquez sur **Delete** (Supprimer).

Étape 3 (Facultatif) Pour être informé lorsqu'une nouvelle clé d'hôte est détectée, cochez la case **Inform me when a new host key is detected** (M'informer lorsqu'une nouvelle clé d'hôte est détectée).

Par défaut, cette option est activée. Lorsque cette option est activée, vous êtes invité à accepter ou à refuser la clé d'hôte si elle n'est pas déjà stockée sur l'ASA. Lorsque cette option est désactivée, l'ASA accepte automatiquement la clé d'hôte si elle n'a pas été stockée auparavant.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer le chemin du client TFTP pour l'ASA

Le TFTP est un protocole de transfert de fichiers client/serveur simple, qui est décrit dans les RFC 783 et RFC 1350, version 2. Vous pouvez configurer l'ASA en tant que client TFTP afin qu'il puisse copier des fichiers vers ou à partir d'un serveur TFTP. De cette façon, vous pouvez sauvegarder et propager des fichiers de configuration sur plusieurs ASA.

Cette section vous permet de prédéfinir le chemin d'accès à un serveur TFTP afin de ne pas avoir à le saisir dans des commandes telles que **copy** et **configure net**.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **File Access (Accès au fichier)** > **TFTP Client (Client TFTP)** et cochez la case **Enable** (Activer).

Étape 2 Dans la liste déroulante Interface Name (Nom de l'interface), choisissez l'interface à utiliser comme client TFTP.

Étape 3 Dans le champ IP Adress (Adresse IP), saisissez l'adresse IP du serveur TFTP sur lequel les fichiers de configuration seront enregistrés.

Étape 4 Dans le champ Path (Chemin), saisissez le chemin d'accès au serveur TFTP sur lequel les fichiers de configuration seront enregistrés.

Par exemple : /tftpboot/asa/config3

Étape 5 Cliquez sur **Apply**.

Ajouter des points de montage

Vous pouvez ajouter un point de montage CIFS ou FTP.

Ajouter un point de montage CIFS

Pour définir un point de montage Common Internet File System (CIFS), procédez comme suit.

Procédure

Étape 1 Sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **File Access (Accès au fichier)** > **Mount-Points (Points de montage)**, et cliquez sur **Add (Ajouter)** > **CIFS Mount Point (Point de montage CIFS)**.

La boîte de dialogue Add CIFS Mount Point (Ajouter un point de montage CIFS) apparaît.

Étape 2 Cochez la case **Enable mount point** (Activer le point de montage).

Cette option associe le système de fichiers CIFS de l'ASA à l'arborescence de fichiers UNIX.

Étape 3 Dans le champ Mount Point Name (Nom du point de montage), saisissez le nom d'un emplacement CIFS existant.

Étape 4 Dans le champ Server Name or IP Address (Nom de serveur ou adresse IP), saisissez le nom ou l'adresse IP du serveur sur lequel se trouve le point de montage.

Étape 5 Dans le champ Share Name (Nom de partage), saisissez le nom du dossier sur le serveur CIFS.

Étape 6 Dans le champ NT Domain Name (Nom de domaine NT), saisissez le nom du domaine NT dans lequel se trouve le serveur.

Étape 7 Dans le champ User Name (Nom d'utilisateur), saisissez le nom de l'utilisateur autorisé pour le montage du système de fichiers sur le serveur.

Étape 8 Dans le champ Password (Mot de passe), saisissez le mot de passe de l'utilisateur autorisé pour le montage du système de fichiers sur le serveur.

Étape 9 Dans le champ Confirm Password (Confirmer le mot de passe), ressaisissez le mot de passe.

Étape 10 Cliquez sur **OK**.

La boîte de dialogue Add CIFS Mount Point (Ajouter un point de montage CIFS) se ferme.

Étape 11 Cliquez sur **Apply** (Appliquer).

Ajouter un point de montage FTP

Pour un point de montage FTP, le serveur FTP doit avoir un style de listage des répertoires UNIX. Les serveurs FTP de Microsoft ont une valeur par défaut du style de listage des répertoires MS-DoS.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **File Access (Accès au fichier)** > **Mount-Points (Points de montage)**, et cliquez sur **Add (Ajouter)** > **FTP Mount Point (Point de montage FTP)**.

La boîte de dialogue Add FTP Mount Point (Ajouter un point de montage FTP) apparaît.

Étape 2 Cochez la case **Enable** (activer).

Cette option associe le système de fichiers FTP de l'ASA à l'arborescence de fichiers UNIX.

Étape 3 Dans le champ Mount Point Name (Nom du point de montage), saisissez le nom d'un emplacement FTP existant.

Étape 4 Dans le champ Server Name or IP Address (Nom de serveur ou adresse IP), saisissez le nom ou l'adresse IP du serveur où se trouve le point de montage.

Étape 5 Dans le champ Mode, cliquez sur le bouton radio du mode FTP (**Actif** ou **Passif**). Lorsque vous choisissez le mode passif, le client initie à la fois la connexion de contrôle FTP et la connexion de données. Le serveur répond par le numéro de son port d'écoute pour cette connexion.

Étape 6 Dans le champ Path to Mount (Chemin d'accès au montage), saisissez le nom du chemin d'accès au répertoire du serveur de fichiers FTP.

Étape 7 Dans le champ User Name (Nom d'utilisateur), saisissez le nom de l'utilisateur autorisé pour le montage du système de fichiers sur le serveur.

Étape 8 Dans le champ Password (Mot de passe), saisissez le mot de passe de l'utilisateur autorisé pour le montage du système de fichiers sur le serveur.

Étape 9 Dans le champ Confirm Password (Confirmer le mot de passe), ressaisissez le mot de passe.

Étape 10 Cliquez sur **OK**.

La boîte de dialogue Add FTP Mount Point (Ajouter un point de montage FTP) se ferme.

Étape 11 Cliquez sur **Apply** (Appliquer).

Accéder à l'outil de gestion de fichiers

Pour utiliser les outils de gestion de fichiers, procédez comme suit.

Procédure

Étape 1 Dans la fenêtre d'application principale d'ASDM, choisissez **Tools (Outils)** > **File Management (Gestion des fichiers)**.

La boîte de dialogue File Management (Gestion des fichiers) apparaît.

- Le volet Folders (Dossiers) affiche les dossiers disponibles sur le disque.
- Le champ Flash Space (Espace flash) affiche la quantité totale de mémoire flash et la quantité de mémoire disponible.
- La zone Files (Fichiers) affiche les renseignements suivants sur les fichiers du dossier sélectionné :
  - Path
  - Filename
  - Taille (octets)
  - Heure de modification
  - Status (État), qui indique si un fichier sélectionné est désigné comme fichier de configuration de démarrage, fichier image de démarrage, fichier image ASDM, fichier image SVC, fichier image CSD ou fichier image APCF.

Étape 2 Cliquez sur **View** (Afficher) pour afficher le fichier sélectionné dans votre navigateur.

Étape 3 Cliquez sur **Cut** (Couper) pour couper le fichier sélectionné afin de le coller dans un autre répertoire.

Étape 4 Cliquez sur **Copy** (Copier) pour copier le fichier sélectionné afin de le coller dans un autre répertoire.

Étape 5 Cliquez sur **Paste** (Coller) pour coller le fichier copié dans la destination sélectionnée.

Étape 6 Cliquez sur **Delete** (Supprimer) pour supprimer le fichier sélectionné de la mémoire flash.

Étape 7 Cliquez sur **Rename** (Renommer) pour renommer un fichier.

Étape 8 Cliquez sur **New Directory** (Nouveau répertoire) pour créer un nouveau répertoire pour le stockage des fichiers.

Étape 9 Cliquez sur **File Transfer** (Transfert de fichiers) pour ouvrir la boîte de dialogue de transfert de fichiers. Consultez Transférer des fichiers, à la page 1198 pour de plus amples renseignements.

Étape 10 Cliquez sur **Support Points** (Points de montage) pour ouvrir la boîte de dialogue Manage Mount Points (Gérer les points de montage). Consultez Ajouter des points de montage, à la page 1196 pour de plus amples renseignements.

Transférer des fichiers

L'outil de transfert de fichiers vous permet de transférer des fichiers à partir d'un emplacement local ou distant. Vous pouvez transférer un fichier local sur votre ordinateur ou un système de fichiers flash vers et à partir de

l'ASA. Vous pouvez transférer un fichier distant vers et à partir de l'ASA en utilisant HTTP, HTTPS, TFTP, FTP ou SMB.

Remarque Pour le module logiciel IPS SSP, avant de télécharger le logiciel IPS sur disk0, assurez-vous qu'au moins 50 % de la mémoire flash est libre. Lorsque vous installez IPS, IPS réserve 50 % de la mémoire flash interne pour son système de fichiers.

Transférer des fichiers entre l'ordinateur local et la mémoire flash

Pour transférer des fichiers entre votre ordinateur local et un système de fichiers flash, procédez comme suit.

Procédure

Étape 1 Dans la fenêtre d'application principale d'ASDM, choisissez **Tools (Outils)** > **File Management (Gestion des fichiers)**.

La boîte de dialogue File Management (Gestion des fichiers) apparaît.

Étape 2 Cliquez sur la flèche vers le bas à côté de **File Transfer** (Transfert de fichiers), puis cliquez sur **Between Local PC and Flash** (Entre l'ordinateur local et la mémoire flash).

La boîte de dialogue File Transfer (Transfert de fichiers) apparaît.

Étape 3 Sélectionnez et *faites glisser* le ou les fichiers depuis votre ordinateur local ou le système de fichiers flash que vous souhaitez charger ou télécharger vers l'emplacement souhaité. Vous pouvez également sélectionner les fichiers sur votre ordinateur local ou sur le système de fichiers flash que vous souhaitez charger ou télécharger, puis cliquer sur la flèche de droite ou de gauche pour transférer ces fichiers vers l'emplacement souhaité.

Étape 4 Cliquez sur **Close** (Fermer) lorsque vous avez terminé.

Transférer des fichiers entre le serveur distant et la mémoire flash

Pour transférer des fichiers entre un serveur distant et un système de fichiers flash, procédez comme suit.

Procédure

Étape 1 Dans la fenêtre d'application principale d'ASDM, choisissez **Tools (Outils)** > **File Management (Gestion des fichiers)**.

La boîte de dialogue File Management (Gestion des fichiers) apparaît.

Étape 2 Cliquez sur la flèche vers le bas dans la liste déroulante File Transfer (Transfert de fichiers), puis cliquez sur **Between Remote Server and Flash** (Entre le serveur distant et la mémoire flash).

La boîte de dialogue File Transfer (Transfert de fichiers) apparaît.

Étape 3 Pour transférer un fichier d'un serveur distant, cliquez sur l'option **Remote server** (Serveur distant).

Étape 4 Définissez le fichier source à transférer.

a) (Facultatif) Spécifiez l'interface par laquelle l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.

b) Choisissez le chemin d'accès à l'emplacement du fichier, y compris l'adresse IP du serveur.



Remarque Le transfert de fichiers prend en charge les adresses IPv4 et IPv6.

c) Saisissez le type (si le chemin est FTP) ou le numéro de port (si le chemin est HTTP ou HTTPS) du serveur distant. Les types de FTP valides sont les suivants :

- ap : fichiers ASCII en mode passif
- an : fichiers ASCII en mode non passif
- ip : fichiers image binaires en mode passif
- in : fichiers image binaires en mode non passif

Étape 5 Pour transférer le fichier à partir du système de fichiers flash, cliquez sur l'option **Flash file system** (Système de fichiers flash).

Étape 6 Saisissez le chemin d'accès à l'emplacement du fichier ou cliquez sur **Browse Flash** (Parcourir la mémoire flash) pour trouver l'emplacement du fichier.

Étape 7 En outre, vous pouvez copier un fichier à partir de votre configuration de démarrage, de la configuration en cours d'exécution ou d'un système de fichiers SMB au moyen de l'interface de ligne de commande. Pour obtenir des instructions sur l'utilisation de la commande **copy**, consultez le guide de configuration de l'interface de ligne de commande.

Étape 8 Définissez la destination du fichier à transférer.

a) Pour transférer le fichier dans le système de fichiers flash, choisissez l'option **Flash file system** (Système de fichiers flash).

b) Saisissez le chemin d'accès à l'emplacement du fichier ou cliquez sur **Browse Flash** (Parcourir la mémoire flash) pour trouver l'emplacement du fichier.

Étape 9 Pour transférer un fichier vers un serveur distant, sélectionnez l'option **Remote server** (Serveur distant).

a) (Facultatif) Spécifiez l'interface par laquelle l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.

b) Saisissez le chemin d'accès à l'emplacement du fichier.

c) Pour les transferts FTP, saisissez le type. Les types valides sont les suivants :

- ap : fichiers ASCII en mode passif
- an : fichiers ASCII en mode non passif
- ip : fichiers image binaires en mode passif
- in : fichiers image binaires en mode non passif

Étape 10 Cliquez sur **Transfer** (Transférer) pour commencer le transfert de fichiers.

La boîte de dialogue Enter Username and Password (Saisir le nom d'utilisateur et le mot de passe) apparaît.

Étape 11 Saisissez le nom d'utilisateur, le mot de passe et le domaine (si nécessaire) pour le serveur distant.

Étape 12 Cliquez sur **OK** pour continuer le transfert de fichiers.

Le processus de transfert de fichiers peut prendre quelques minutes; assurez-vous d'attendre la fin de l'opération.

Étape 13 Cliquez sur **Close** (Fermer) lorsque le transfert de fichiers est terminé.

Définir l'image ASA, ASDM et la configuration de démarrage

Si vous avez plus d'une image ASA ou ASDM, vous devez spécifier l'image que vous souhaitez démarrer. Si vous ne définissez pas l'image, l'image de démarrage par défaut est utilisée et cette image peut ne pas être celle prévue. Pour la configuration de démarrage, vous pouvez éventuellement spécifier un fichier dans le système de fichiers visible au lieu d'un répertoire masqué.

Voir les directives suivantes concernant les modèles :

- Châssis Firepower 4100/9300 : les mises à niveau ASA sont gérées par FXOS; vous ne pouvez pas mettre à niveau l'ASA dans le système d'exploitation de l'ASA, donc n'utilisez pas cette procédure pour l'image de l'ASA. Vous pouvez mettre à niveau ASA et FXOS séparément, car ils sont répertoriés séparément dans la liste du répertoire FXOS. L'ensemble ASA comprend toujours ASDM.
- Firepower 2100 en mode plateforme : les images ASA, ASDM et FXOS sont regroupées en un seul ensemble. Les mises à jour de paquets sont gérées par FXOS; vous ne pouvez pas mettre à niveau l'ASA dans le système d'exploitation de l'ASA, donc n'utilisez pas cette procédure pour l'image de l'ASA. Vous *ne pouvez pas* mettre à niveau ASA et FXOS séparément; ils sont toujours regroupés.
- Firepower 1000, 2100 en mode d'appareil, Secure Firewall 3100 : les images ASA, ASDM et FXOS sont regroupées en un seul paquet. Les mises à jour de paquets sont gérées par l'ASA à l'aide de cette procédure. Bien que ces plateformes utilisent l'ASA pour identifier l'image à démarrer, le mécanisme sous-jacent est différent de celui des ASA existants. Consultez la description de la commande ci-dessous pour plus d'informations.
- ASDM pour les modèles : ASDM peut être mis à niveau à partir du système d'exploitation de l'ASA, de sorte que vous n'avez pas besoin d'utiliser uniquement l'image ASDM fournie. Pour Firepower 2100 en mode plateforme et Firepower 4100/9300, les images ASDM que vous téléchargez manuellement ne s'affichent pas dans la liste d'images FXOS; vous devez les gérer à partir de l'ASA.



Remarque Lorsque vous mettez à niveau le paquet de l'ASA, l'image ASDM de l'offre groupée remplace l'image du groupe ASDM précédent sur l'ASA, car elles portent le même nom (**asdm.bin**). Toutefois, si vous avez choisi manuellement une autre image ASDM que vous avez téléversée (par exemple, **asdm-782.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'exécuter une version compatible d'ASDM, vous devez soit mettre à niveau ASDM avant de mettre à niveau l'ensemble, soit reconfigurer l'ASA pour utiliser l'image ASDM fournie (**asdm.bin**) juste avant de mettre à niveau l'ensemble ASA.

- ASA virtuel : le paquet de déploiement initial ASA virtuel place l'image de l'ASA dans la partition boot:/ en lecture seule. Lorsque vous mettez à niveau ASA virtuel, vous spécifiez une image différente dans la mémoire flash. Notez que si vous effacez votre configuration ultérieurement avec la commande, l' ASA virtuel reviendra au chargement de l'image de déploiement d'origine. Le paquet de déploiement initial ASA virtuel comprend également une image ASDM qu'il place dans la mémoire flash. Vous pouvez mettre à niveau l'image ASDM séparément.
- **disk0:** est la mémoire interne. D'autres numéros de lecteur représentent un stockage externe tel qu'un lecteur USB, un SSD ou une carte SD.

Consultez les paramètres par défaut suivants :

- Image ASA :
  - Firepower 1000, 2100 en mode d'appareil,1200/3100/4200 : démarre l'image de démarrage précédente.
  - ISA 3000 : démarre la première image d'application trouvée dans la mémoire flash interne.
  - ASA virtuel : démarre l'image dans la partition boot:/ en lecture seule qui a été créée lors du déploiement initial.
  - Châssis Firepower 4100/9300 : le système FXOS détermine quelle image ASA démarrer. Vous ne pouvez pas utiliser cette procédure pour définir l'image ASA.
  - Firepower 2100 en mode plateforme : le système FXOS détermine quel paquet ASA/FXOS démarrer. Vous ne pouvez pas utiliser cette procédure pour définir l'image ASA.
- Image ASDM sur tous les ASA : démarre la première image ASDM qu'il trouve dans la mémoire flash interne ou, si elle n'en existe pas à cet emplacement, dans la mémoire flash externe.
- Configuration de démarrage : par défaut, l'ASA démarre à partir d'une configuration de démarrage qui est un fichier masqué.

Procédure

Étape 1 Choisissez **Configuration** > **Management** > **System Image/Configuration** > **Boot Image/Configuration**.

Firepower 1000, 2100 en mode l'appareil, Secure : vous ne pouvez ajouter qu'une seule image. Si vous mettez à niveau vers une nouvelle image, vous devrez supprimer l'image précédente que vous avez définie. Lorsque vous appliquez ce changement, le système effectue une action : il valide et décompresse l'image et la copie dans l'emplacement de démarrage (un emplacement interne sur disk0 géré par FXOS). La nouvelle image sera chargée lorsque vous rechargerez l'ASA. Si vous changez d'avis avant de téléverser, vous pouvez supprimer **l'emplacement de l'image de démarrage** et soumettre une nouvelle demande pour supprimer la nouvelle image de l'emplacement de démarrage, de sorte que l'image actuelle continue de s'exécuter. Vous pouvez même supprimer le fichier image d'origine de la mémoire flash de l'ASA après avoir appliqué cette modification, et l'ASA démarrera correctement à partir de l'emplacement de démarrage. Contrairement à d'autres modèles, cette commande dans la configuration de démarrage n'affecte pas l'image de démarrage. La dernière image de démarrage chargée sera toujours exécutée lors du rechargement. Vous pouvez uniquement téléverser des images avec le nom de fichier d'origine à partir du site de téléchargement de Cisco. Si vous modifiez le nom de fichier, il ne se téléversera pas.

Autres modèles : vous pouvez spécifier jusqu'à quatre fichiers images binaires locaux à utiliser comme image de démarrage et une image sur un serveur TFTP à partir du périphérique de démarrage. Si vous spécifiez une image située sur un serveur TFTP, elle doit être la première de la liste. Si le périphérique ne peut pas atteindre le serveur TFTP pour téléverser l'image, il tente de téléverser le fichier image suivant de la liste située dans la mémoire flash.

Étape 2 Cliquez sur **Add** (Ajouter) dans le volet Boot Image/Configuration.

Étape 3 Accédez à l'image à partir de laquelle vous souhaitez démarrer. Pour une image TFTP, saisissez l'URL TFTP dans le champ File Name (nom de fichier). Cliquez sur **OK**.

Étape 4 Disposez les images dans l'ordre à l'aide des boutons de déplacement vers le haut et vers le bas.

Étape 5 (Facultatif) Dans le champ Boot Configuration File Path (chemin d'accès au fichier de configuration de démarrage), précisez le fichier de configuration de démarrage en cliquant sur **Browse Flash** (Parcourir la mémoire flash) et en sélectionnant la configuration. Cliquez sur **OK**.

Cette fonctionnalité est importante lorsque vous travaillez avec des configurations volumineuses qui ne tiennent pas dans le répertoire masqué. Si vous enregistrez une grande configuration et que vous voyez le message d'erreur suivant, veillez à enregistrer la configuration dans un nouveau fichier à l'aide de la commande suivante :

```
%Erreur d'écriture. nvRAM:/startup-config (pas d'espace gauche sur le périphérique :)
```

Étape 6 Dans le champ ASDM Image File Path (chemin d'accès au fichier image ASDM), précisez l'image ASDM en cliquant sur **Browse Flash** et en sélectionnant l'image. Cliquez sur **OK**.

Étape 7 Cliquez sur **Apply** (Appliquer).

Sauvegarde et restauration de configurations ou d'autres fichiers

Nous vous recommandons de faire des sauvegardes régulières de votre configuration et d'autres fichiers système pour éviter les défaillances du système.

Effectuer une sauvegarde ou une restauration complète du système

Ces procédures décrivent comment sauvegarder et restaurer les configurations et les images dans un fichier zip et le transférer sur votre ordinateur local.

Avant d'entreprendre la sauvegarde ou la restauration

- Vous devez avoir au moins 300 Mo d'espace disque disponible à l'emplacement de sauvegarde ou de restauration avant de lancer une sauvegarde ou une restauration.
- L'ASA doit être en mode de contexte unique.
- Vous ne pouvez lancer qu'une seule sauvegarde ou restauration à la fois.
- Si vous apportez des modifications à la configuration pendant ou après une sauvegarde, ces modifications ne seront pas incluses dans la sauvegarde. Si vous modifiez une configuration après avoir effectué la

sauvegarde, puis effectuez une restauration, cette modification de configuration sera remplacée. Par conséquent, l'ASA pourrait se comporter différemment.

- Ne remplacez pas ou ne restaurez pas le fichier de configuration système (*cspCfg.xml*) d'un ASA à un autre, en particulier entre les différents modèles de plateforme ASA. Le fichier *cspCfg.xml* peut contenir des informations sur le matériel propres au périphérique. La copie de ce fichier à partir d'un autre ASA peut créer une incompatibilité matérielle, telle que des différences dans le nombre de cœurs de CPU. Cette incompatibilité peut empêcher l'ASA cible de démarrer correctement et finir par le faire passer en mode Failsafe.
- Vous pouvez uniquement restaurer une configuration sur la même version ASA que celle lorsque vous avez effectué la sauvegarde d'origine. Vous ne pouvez pas utiliser l'outil de restauration pour migrer une configuration d'une version ASA vers une autre. Si une migration de configuration est requise, l'ASA met automatiquement à niveau la configuration de démarrage résidente lorsqu'il charge le nouveau système d'exploitation de l'ASA.
- Si vous utilisez la mise en grappe, vous pouvez uniquement sauvegarder ou restaurer les certificats de configuration de démarrage, de configuration d'exécution et d'identité. Vous devez créer et restaurer une sauvegarde séparément pour chaque unité.
- Si vous utilisez le basculement, vous devez créer et restaurer une sauvegarde séparément pour les unités actives et de secours.
- Si vous définissez une phrase secrète principale pour l'ASA, vous avez besoin de cette phrase secrète principale pour restaurer la configuration de sauvegarde que vous créez avec cette procédure. Si vous ne connaissez pas la phrase secrète principale pour l'ASA, consultez Configurer la phrase secrète principale, à la page 765 pour savoir comment la réinitialiser avant de poursuivre la sauvegarde.
- Si vous importez des données PKCS12 (avec la commande **crypto ca trustpoint**) et que le point de confiance utilise des clés RSA, la paire de clés importée se voit attribuer le même nom que le point de confiance. En raison de cette limite, si vous spécifiez un nom différent pour le point de confiance et sa paire de clés après avoir restauré une configuration ASDM, la configuration de démarrage sera la même que la configuration d'origine, mais la configuration d'exécution comprendra un nom de paire de clés différent. Cela signifie que si vous utilisez des noms différents pour la paire de clés et le point de confiance, vous ne pouvez pas restaurer la configuration d'origine. Pour contourner ce problème, assurez-vous d'utiliser le même nom pour le point de confiance et sa paire de clés.
- Vous ne pouvez pas sauvegarder à l'aide de l'interface de ligne de commande et restaurer à l'aide d'ASDM, ou inversement.
- Chaque fichier de sauvegarde comprend le contenu suivant :
  - Configuration d'exécution
  - Configuration du démarrage
  - Toutes les images de sécurité

    Images de Cisco Secure Desktop et de l'analyse de l'hôte

    Paramètres de Cisco Secure Desktop et de l'analyse de l'hôte

    Images et profils (SVC) deSecure Client (services client sécurisés)

    Personnalisations et transformations (SVC) deSecure Client (services client sécurisés)
  - Certificats d'identité (inclut les paires de clés RSA liées aux certificats d'identité; exclut les clés autonomes)

- Clés prépartagées VPN
- Configurations SSL VPN
- Cadre personnalisé du profil d'application (APCF)
- Signets
- Personnalisations
- Politique d'accès dynamique (DAP)
- Modules d'extension
- Scripts de préremplissage pour les profils de connexion
- Configuration automatique du serveur mandataire
- Table de traduction
- Web content
- Information de version

Sauvegarder le système

Cette procédure décrit comment effectuer une sauvegarde complète du système.



Remarque Si le processus de sauvegarde se bloque, il est possible que votre ASDM ne dispose pas de suffisamment de mémoire pour charger la configuration. Vous pouvez superviser la console Java pour détecter le message « java.lang.OutOfMemoryError » afin de déterminer si le problème est lié à un manque de mémoire. Pour augmenter la mémoire ASDM, consultez Augmenter la mémoire de configuration de l'ASDM, à la page 30.

Procédure

Étape 1 Créez un dossier sur votre ordinateur pour stocker les fichiers de sauvegarde afin qu'ils soient faciles à trouver au cas où vous deviez les restaurer ultérieurement.

Étape 2 Choisissez **Tools (Outils)** > **Backup Configurations (Configurations de sauvegarde)**.

La boîte de dialogue Backup Configurations (Configurations de sauvegarde) s'affiche. Cliquez sur la flèche vers le bas dans la zone **SSL VPN Configuration** (Configuration SSL VPN) pour afficher les options de sauvegarde des configurations SSL VPN. Par défaut, tous les fichiers de configuration sont vérifiés et seront sauvegardés s'ils sont disponibles. Si vous souhaitez sauvegarder tous les fichiers de la liste, passez à l'étape 5.

Étape 3 Décochez la case **Backup All** (Sauvegarder tout) si vous souhaitez sélectionner les configurations à sauvegarder.

Étape 4 Cochez la case à côté de l'option que vous souhaitez sauvegarder.

Étape 5 Cliquez sur **Browse Local (Parcourir local) pour spécifier un répertoire et un nom de fichier pour le fichier de sauvegarde .zip.**

Étape 6 Dans la boîte de dialogue Select (Sélectionner), choisissez le répertoire dans lequel vous souhaitez stocker le fichier de sauvegarde.

Étape 7 Cliquez sur **Select** (sélectionner). Le chemin d'accès apparaît dans le champ Backup File (Fichier de sauvegarde).

Étape 8 Saisissez le nom du fichier de sauvegarde de destination après le chemin d'accès au répertoire. Le nom du fichier de sauvegarde doit comporter entre 3 et 232 caractères.

Étape 9 Cliquez sur **Backup** (Sauvegarde). La sauvegarde se poursuit immédiatement, sauf si vous sauvegardez des certificats ou que l'ASA utilise une phrase secrète principale.

Étape 10 Si vous avez configuré et activé une phrase secrète principale sur votre ASA, vous recevez un message d'avertissement avec une proposition de modification de la phrase secrète principale, si vous ne la connaissez pas, avant de procéder à la sauvegarde. Cliquez sur Yes (Oui) pour poursuivre la sauvegarde si vous connaissez la phrase secrète principale. La sauvegarde se poursuit immédiatement, sauf si vous sauvegardez des certificats d'identité.

Étape 11 Si vous sauvegardez un certificat d'identité, vous devez saisir une phrase secrète distincte à utiliser pour le chiffrement des certificats au format PKCS12. Vous pouvez saisir une phrase secrète ou ignorer cette étape.

Remarque Seuls les certificats d'identité sont sauvegardés par ce processus.

- Pour chiffrer les certificats, saisissez et confirmez votre phrase secrète dans la boîte de dialogue Certificate Passphrase (Phrase secrète du certificat) et cliquez sur OK. Vous devrez vous souvenir du mot de passe que vous avez saisi dans cette boîte de dialogue lors de la restauration des certificats.
- Cliquez sur **Cancel** (Annuler) pour ignorer cette étape et ne pas sauvegarder les certificats.

Après avoir cliqué sur OK ou Cancel (Annuler), la sauvegarde commence immédiatement.

Étape 12 Une fois la sauvegarde terminée, la fenêtre d'état se ferme et la boîte de dialogue Backup Statistics (Statistiques de sauvegarde) apparaît pour afficher des messages de réussite et d'échec.

Remarque Les « messages d'échec » des sauvegardes sont très probablement causés par l'absence de configuration existante pour les types indiqués.

Étape 13 Cliquez sur **OK** pour fermer la boîte de dialogue Backup Statistics (Statistiques de sauvegarde).

Restaurer la sauvegarde

Vous pouvez spécifier les configurations et les images à restaurer à partir d'un fichier zip tar.gz sur votre ordinateur local.

Remarque Si le processus de restauration se bloque, il est possible que votre ASDM ne dispose pas de suffisamment de mémoire pour charger la configuration. Vous pouvez superviser la console Java pour détecter le message « java.lang.OutOfMemoryError » afin de déterminer si le problème est lié à un manque de mémoire. Pour augmenter la mémoire ASDM, consultez Augmenter la mémoire de configuration de l'ASDM, à la page 30.

Procédure

Étape 1 Choisissez **Tools (Outils)** > **Restore Configurations (Restaurer les configurations)**.

Étape 2 Dans la boîte de dialogue Restore Configurations (Restaurer les configurations), cliquez sur **Browse Local Directory** (Parcourir le répertoire local), choisissez le fichier zip sur votre ordinateur local qui contient la configuration à restaurer, puis cliquez sur **Select** (Sélectionner). Le chemin d'accès et le nom du fichier zip apparaissent dans le champ **Local File** (Fichier local).

Le fichier zip que vous restaurez doit être créé en sélectionnant l'option **Tools (Outils) > Backup Configurations (Configurations de sauvegarde)**.

Étape 3 Cliquez sur **Next** (suivant). La boîte de dialogue Restore Configurations (Restaurer les configurations) s'affiche. Cochez les cases en regard des configurations que vous souhaitez restaurer. Toutes les configurations SSL VPN disponibles sont sélectionnées par défaut.

Étape 4 Cliquez sur **Restaurer**.

Étape 5 Si vous avez spécifié une phrase secrète pour chiffrer les certificats lors de la création du fichier de sauvegarde, ASDM vous invite à saisir cette phrase secrète.

Étape 6 Si vous avez choisi de restaurer la configuration en cours d'exécution, il vous est demandé si vous souhaitez fusionner la configuration en cours d'exécution, remplacer la configuration en cours d'exécution ou ignorer cette partie du processus de restauration.

- La fusion des configurations combine la configuration en cours d'exécution actuelle et la configuration en cours d'exécution sauvegardée.
- Le remplacement de la configuration en cours d'exécution utilise uniquement la configuration en cours d'exécution sauvegardée.
- Ignorer cette étape ne restaure pas la configuration en cours d'exécution sauvegardée.

ASDM affiche une boîte de dialogue d'état jusqu'à ce que l'opération de restauration soit terminée.

Étape 7 Si vous avez remplacé ou fusionné la configuration en cours d'exécution, fermez ASDM et redémarrez-le. Si vous n'avez pas restauré la configuration en cours d'exécution, actualisez la session ASDM pour que les modifications prennent effet.

Configurer la sauvegarde et la restauration automatiques (ISA 3000)

Sur l'ISA 3000, vous pouvez configurer des sauvegardes automatiques vers un emplacement particulier chaque fois que vous enregistrez votre configuration.

La restauration automatique vous permet de configurer facilement de nouveaux périphériques avec une configuration complète chargée sur une carte de mémoire flash SD. La restauration automatique est activée dans la configuration d'usine par défaut.

Configurer la sauvegarde automatique (ISA 3000)

Sur l'ISA 3000, vous pouvez configurer des sauvegardes automatiques vers un emplacement particulier chaque fois que vous enregistrez votre configuration.

Avant de commencer

Cette fonctionnalité est uniquement disponible sur l'ISA 3000.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Auto Backup and Restore Configuration (Configuration de la sauvegarde et de la restauration automatiques)**.

Étape 2 Cochez ou décochez la case **Automate Backup Configuration** (Automatiser la configuration de la sauvegarde) pour activer ou désactiver les sauvegardes automatiques.

Si vous activez les sauvegardes automatiques, lorsque vous enregistrez la configuration, la configuration est automatiquement enregistrée à l'emplacement de sauvegarde ainsi que dans la configuration de démarrage. Le fichier de sauvegarde est intitulé « auto-backup-asa.tgz ».

Définissez les paramètres suivants :

- **Interface** : spécifie l'interface permettant d'atteindre l'URL de sauvegarde, si vous spécifiez un stockage hors périphérique. Si vous ne spécifiez pas de nom d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.
- **Location** (Emplacement) : spécifie le support de stockage à utiliser pour la sauvegarde des données. Vous pouvez définir une URL ou un stockage local. disk0 est le lecteur flash interne, disk1 est une clé de mémoire USB facultative sur USB 1 et disk2 est une clé de mémoire USB facultative sur USB 2. Et disk3 est la carte mémoire SD. La valeur par défaut pour la restauration automatique est disk3.
- **Passphrase** (Phase secrète) : définit la phrase secrète pour sécuriser les données sauvegardées. La valeur par défaut pour la restauration automatique est « cisco ».

Configurer la restauration automatique (ISA 3000)

Le mode de restauration automatique restaure la configuration système sur un périphérique sans intervention de l'utilisateur. Par exemple, vous insérez une carte de mémoire SD contenant une configuration de sauvegarde enregistrée dans un nouveau périphérique, puis mettez celui-ci sous tension. Lorsque le périphérique se manifeste, il vérifie la carte SD pour décider si la configuration système doit être restaurée. (La restauration n'est lancée que si le fichier de sauvegarde comporte l'« empreinte digitale » d'un autre périphérique. L'empreinte du fichier de sauvegarde est mise à jour pour correspondre au périphérique actuel lors d'une opération de sauvegarde ou de restauration. Donc, si le périphérique a déjà effectué une restauration ou s'il a créé sa propre sauvegarde, la restauration automatique est ignorée.) Si l'empreinte indique qu'une restauration est requise, le périphérique remplace la configuration système (startup-config, running-config, configuration du SSL VPN, etc.; consultez Sauvegarder le système, à la page 1205 pour plus de détails sur le contenu de la sauvegarde). Lorsque le périphérique a terminé son démarrage, il exécute la configuration enregistrée.

La restauration automatique est activée dans la configuration d'usine par défaut. Vous pouvez donc facilement configurer de nouveaux périphériques avec une configuration complète chargée sur une carte de mémoire SD sans avoir à effectuer de préconfiguration du périphérique.

Étant donné que le périphérique doit décider dès le début du processus de démarrage si la configuration système doit être restaurée, il vérifie les variables ROMMON pour déterminer si le périphérique est en mode de restauration automatique et pour obtenir l'emplacement de la configuration de sauvegarde. Les variables ROMMON suivantes sont utilisées :

- **RESTORE_MODE =** {**auto** | **manual**}

  La valeur par défaut est **auto**.

- **RESTORE_LOCATION =** {**disk0:** | **disk1:** | **disk2:** | **disk3:**}

  La valeur par défaut est **disk3:**.

- **RESTORE_PASSPHRASE** = *key*

  La valeur par défaut est **cisco**.

Pour modifier les paramètres de restauration automatique, procédez comme suit.

Avant de commencer

- Cette fonctionnalité est uniquement disponible sur l'ISA 3000.
- Si vous utilisez les paramètres de restauration par défaut, une carte de mémoire SD doit être installée (numéro de pièce SD-IE-1GB=).
- Si vous devez restaurer la configuration par défaut pour vous assurer que la restauration automatique est activée, utilisez la commande **configure factory default**. Cette commande est uniquement disponible en mode de pare-feu transparent. Par conséquent, si vous êtes en mode de pare-feu routé, utilisez d'abord la commande **firewall transparent**.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Auto Backup and Restore Configuration (Configuration de la sauvegarde et de la restauration automatiques)**.

Étape 2 Cochez ou décochez la case **Automate Restore Configuration** (Automatiser la configuration de la restauration) pour activer ou désactiver la restauration automatique.

Le nom du fichier restauré est « auto-backup-asa.tgz ». Si vous activez la restauration automatique, définissez les paramètres suivants :

- **Location** (Emplacement) : spécifie le support de stockage à utiliser pour la restauration des données. disk0 est le lecteur flash interne, disk1 est une clé de mémoire USB facultative sur USB 1 et disk2 est une clé de mémoire USB facultative sur USB 2. Et disk3 est la carte mémoire SD. La valeur par défaut est disk3.
- **Passphrase** (Phase secrète) : définit la phrase secrète pour lire les données sauvegardées. La valeur par défaut est « cisco ».

Enregistrer la configuration en cours d'exécution sur un serveur TFTP

Cette fonctionnalité stocke une copie du fichier de configuration en cours d'exécution sur un serveur TFTP.

Procédure

Étape 1 Choisissez **File (Fichier)** > **Save Running Configuration to TFTP Server (Enregistrer la configuration en cours d'exécution sur un serveur TFTP)**.

La boîte de dialogue Save Running Configuration to TFTP Server (Enregistrer la configuration en cours d'exécution sur le serveur TFTP) s'affiche.

Étape 2 Saisissez l'adresse IP du serveur TFTP et le chemin d'accès au fichier sur le serveur TFTP dans lequel le fichier de configuration sera enregistré, puis cliquez sur **Save Configuration** (Enregistrer la configuration).

Remarque Pour configurer les paramètres TFTP par défaut, choisissez **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > TFTP Client (Client TFTP)**. Après avoir configuré ce paramètre, l'adresse IP du serveur TFTP et le chemin d'accès au fichier sur le serveur TFTP s'affichent automatiquement dans cette boîte de dialogue.

Programmer un redémarrage du système

L'outil System Reload (Rechargement du système) vous permet de planifier le redémarrage du système ou d'annuler un redémarrage en attente.

Procédure

Étape 1 Choisissez **Tools (Outils)** > **System Reload (Rechargement du système)**.

Étape 2 Dans la zone Reload Scheduling (Planification du rechargement), définissez les paramètres suivants :

a) Pour l'état de configuration, choisissez d'enregistrer ou de supprimer la configuration en cous d'exécution au redémarrage.

b) Pour l'heure de début du rechargement, choisissez parmi les options suivantes :

- Cliquez sur **Now** (Maintenant) pour effectuer un redémarrage immédiat.
- Cliquez sur **Delay by** (Retarder de) pour retarder le redémarrage d'une durée spécifiée. Saisissez le temps avant que le redémarrage ne commence, en heures et en minutes ou en minutes seulement.
- Cliquez sur **Schedule at** (Planifier à) pour planifier le redémarrage à une heure et à une date précises. Saisissez l'heure du jour à laquelle le redémarrage doit se produire et sélectionnez la date du redémarrage planifié.

c) Dans le champ Reload Message (Recharger le message), saisissez un message à envoyer aux instances ouvertes d'ASDM au redémarrage.

d) Cochez la case **On reload failure force immediate reload after** (En cas d'échec du rechargement, forcer un rechargement immédiat après) pour afficher le temps écoulé en heures et en minutes ou seulement en minutes avant de retenter un redémarrage.
e) Cliquez sur **Schedule Reload** (Planifier le rechargement) pour planifier le redémarrage comme configuré.

La zone Reload Status (État du rechargement) affiche l'état du redémarrage.

Étape 3 Effectuez l'une des opérations suivantes :

- Cliquez sur **Cancel Reload** (Annuler le rechargement) pour arrêter un redémarrage planifié.
- Cliquez sur **Refresh** (Actualiser) pour actualiser l'affichage de l'état du rechargement une fois le redémarrage planifié terminé.
- Cliquez sur **Details** (Détails) pour afficher les résultats d'un redémarrage planifié.

Échange à chaud d'un SSD sur Cisco Secure Firewall

Si vous avez deux disques SSD, ils forment un RAID lorsque vous démarrez. Vous pouvez effectuer les tâches suivantes au niveau de l'interface de ligne de commande lorsque le pare-feu est sous tension :

- Échangez à chaud un des disques SSD : si un disque SSD est défectueux, vous pouvez le remplacer. Notez que si vous n'avez qu'un seul disque SSD, vous ne pouvez pas le retirer tant que le pare-feu est sous tension.
- Retirez un des disques SSD : si vous avez deux disques SSD, vous pouvez en retirer un.
- Ajouter un deuxième SSD : si vous avez un deuxième SSD, vous pouvez en ajouter un deuxième et former un RAID.

  Lorsque vous utilisez un seul disque SSD dans les périphériques Secure Firewall, l' **état du disque** indiquera **détérioré**.



Mise en garde Ne retirez pas physiquement un SSD sans l'avoir supprimé du RAID en suivant cette procédure. Vous pourriez entraîner des pertes de données.

Procédure

Étape 1 Retirez l'un des disques SSD.

a) Retirez le SSD du RAID.

raid remove-secure local-disk {**1** | **2**}

Le mot clé **remove-secure** supprime le SSD du RAID, désactive la fonction de disque à chiffrement automatique et effectue un effacement sécurisé du SSD. Si vous souhaitez uniquement retirer le SSD du RAID et conserver les données intègres, vous pouvez utiliser le mot clé **remove**.

Exemple :

```
ciscoasa(config)# raid remove-secure local-disk 2
```

b) Surveiller l'état RAID jusqu'à ce que SSD ne s'affiche plus dans l'inventaire.

show raid

Une fois le SSD retiré du RAID, l'**exploitabilité** et **l'état du lecteur** s'affichent comme **dégradés**. Le deuxième lecteur ne sera plus répertorié en tant que disque membre.

Exemple :

```
ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
```

```
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) Retirez physiquement le disque SSD du châssis.

Étape 2 Ajouter un disque SSD.

a) Ajoutez physiquement le SSD dans le logement vide.

b) Ajoutez le SSD au RAID.

raid add local-disk {**1** | **2**}

La synchronisation du nouveau SSD avec le RAID peut prendre plusieurs heures, pendant laquelle le pare-feu est complètement opérationnel. Vous pouvez même redémarrer et la synchronisation se poursuivra après la mise sous tension. Utilisez la commande **show raid** pour afficher l'état.

Si vous installez un disque SSD qui a été utilisé précédemment sur un autre système et qui est toujours verrouillé, saisissez la commande suivante :

raid add local-disk {**1** | **2**} *psid*

Le *psid* est imprimé sur l'étiquette fixée à l'arrière du disque SSD. Sinon, vous pouvez redémarrer le système et le SSD sera formaté et ajouté au RAID.

Historique des logiciels et des configurations

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Client et serveur Secure Copy	9.1(5)/9.2(1)	L'ASA prend désormais en charge le client et le serveur Secure Copy (SCP) pour transférer des fichiers vers et depuis un serveur SCP. Nous avons modifié les écrans suivants : Tools (Outils) > File Management (Gestion des fichiers) > File Transfer (Transfert de fichiers) > Between Remote Server and Flash (Entre le serveur distant et la configuration flash) **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès aux fichiers) > Secure Copy (SCP) Server (Serveur Secure Copy (SCP))**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Chiffrement SSH et d'intégrité configurables	9.1(7)/9.4(3)/9.5(3)/9.6(1)	Les utilisateurs peuvent sélectionner des modes de chiffrement lors de la gestion du chiffrement SSH et peuvent configurer le HMAC et le chiffrement pour divers algorithmes d'échange de clés. Vous souhaiterez peut-être modifier les chiffres pour qu'ils soient plus ou moins stricts, selon votre application. Notez que la performance de la copie sécurisée dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier les chiffres proposés, utilisez **ssh cipher encryption custom aes128-cbc**, par exemple. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffres SSH)**
Vérification du certificat du serveur de mise à jour automatique activée par défaut	9.2(1)	La vérification du certificat du serveur de mise à jour automatique est maintenant activée par défaut; pour les nouvelles configurations, vous devez explicitement désactiver la vérification de certificat. Si vous effectuez une mise à niveau à partir d'une version antérieure et que vous n'avez pas activé la vérification de certificat, la vérification de certificat n'est pas activée, et l'avertissement suivant s'affiche : `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` La configuration sera migrée vers la configuration explicite sans vérification. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > System/Image Configuration (Configuration système/image) > Auto Update (Mise à jour automatique) > Add Auto Update Server (Ajouter l'Auto Update Server).
Sauvegarde et restauration du système à l'aide de l'interface de ligne de commande	9.3(2)	Vous pouvez maintenant sauvegarder et restaurer des configurations système complètes, y compris les images et les certificats, à l'aide de l'interface de ligne de commande. Nous n'avons pas modifié d'écrans ASDM.
Récupération et chargement d'une nouvelle image ASA 5506W-X	9.4(1)	Nous prenons désormais en charge la récupération et le chargement d'une nouvelle image ASA 5506W-X. Nous n'avons pas modifié d'écrans ASDM.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Sauvegarde et restauration automatiques pour l'ISA 3000	9.7(1)	Vous pouvez activer la fonction de sauvegarde automatique et/ou de restauration automatique en utilisant les paramètres prédéfinis dans les commandes de sauvegarde et de restauration. Les scénarios de ces fonctionnalités comprennent la configuration initiale à partir d'un support externe; le remplacement de l'appareil; la restauration à un état opérationnel. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Auto Backup and Restore Configuration (Configuration de la sauvegarde et de la restauration automatiques)**
La pile CiscoSSH requiert un accès SSH lors de l'utilisation du client SCP	9.17(1)	Si vous utilisez la pile CiscoSSH, ou utilisez la commande ASA **copy** de l'ASA pour copier un fichier vers ou à partir d'un serveur SCP, vous devez activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP
Prise en charge RAID pour les SSD sur le pare-feu Secure Firewall 3100	9.17(1)	Les disques SSD sont des disques à chiffrement automatique (SED), et si vous avez deux disques SSD, ils forment un RAID logiciel. Commandes nouvelles ou modifiées : **raid, show raid, show ssd**



CHAPITRE 46

Automatisation de la réponse pour les événements système

Ce chapitre décrit comment configurer le gestionnaire d'événements intégré (EEG)

- À propos de l'EEG, à la page 1217
- Lignes directrices pour l'EEG, à la page 1219
- Configurer l'EEG, à la page 1219
- Supervision de l'EEG, à la page 1223
- Historique de l'EEG, à la page 1223

À propos de l'EEG

Le service EEG vous permet de déboguer les problèmes et fournit une journalisation à usage général pour le dépannage. Il y a deux composants : les événements auxquels l'EEG répond ou écoute, et les applets de gestionnaire d'événements qui définissent les actions ainsi que les événements auxquels l'EEG répond. Vous pouvez configurer plusieurs applets de gestionnaire d'événements pour répondre à différents événements et effectuer des actions différentes.

Événements pris en charge

L'EEG prend en charge les événements suivants :

- Journal système : l'ASA utilise les ID des messages de journal système pour identifier les messages de journal système qui déclenchent un applet de gestionnaire d'événements. Vous pouvez configurer plusieurs événements de journal système, mais les ID des messages de journal système ne peuvent pas se chevaucher dans un seul applet de gestionnaire d'événements.
- Minuteries : vous pouvez utiliser des minuteries pour déclencher des événements. Vous ne pouvez configurer chaque minuterie qu'une seule fois pour chaque applet de gestionnaire d'événements. Chaque applet de gestionnaire d'événements peut avoir jusqu'à trois minuteries. Les trois types de minuteries sont les suivants :
  - Les minuteries de surveillance (périodiques) déclenchent un applet de gestionnaire d'événements après la période spécifiée suivant la fin des actions de l'applet et redémarrent automatiquement.

- Les minuteries de compte à rebours (à usage unique) déclenchent un applet de gestionnaire d'événements une fois après la période spécifiée et ne redémarrent pas à moins d'être supprimées, puis rajoutées.
- Les minuteries absolues (une fois par jour) déclenchent un événement une fois par jour à une heure spécifiée et redémarrent automatiquement. Le format de l'heure du jour hh:mm:ss.

  Vous ne pouvez configurer qu'un seul événement de minuterie de chaque type pour chaque applet de gestionnaire d'événements.

- Aucun : l'événement Aucun est déclenché lorsque vous exécutez un applet de gestionnaire d'événements manuellement à l'aide de l'interface de ligne de commande ou d'ASDM.
- Plantage : l'événement de plantage est déclenché lorsque l'ASA tombe en panne. Dans certains scénarios, un plantage forcé est déclenché :

  Si l'ASA est configuré pour se recharger en cas d'épuisement du bloc et que l'ASA reste à court de mémoire pendant une durée configurée, il envoie le journal système et recueille des données de dépannage. L'ASA force le plantage et déclenche le processus de rechargement pour libérer le bloc de mémoire. Dans une configuration à haute disponibilité, dans de tels cas, le basculement est déclenché. Dans une configuration de grappe, le nœud quitte la grappe.

  Quelle que soit la valeur de la commande **output**, les commandes **action** sont dirigées vers le fichier crashinfo. La sortie est générée avant la commande **show tech**.

Actions sur les applets de gestionnaire d'événements

Lorsqu'un applet de gestionnaire d'événements est déclenché, les actions sur cet applet sont effectuées. Chaque action a un numéro utilisé pour spécifier la séquence des actions. Le numéro de séquence doit être unique dans un applet de gestionnaire d'événements. Vous pouvez configurer plusieurs actions pour un applet de gestionnaire d'événements. Les commandes sont des commandes d'interface de ligne de commande typiques, telles que **show blocks**.

Destinations de sortie

Vous pouvez envoyer le résultat des actions à un emplacement spécifié à l'aide de la commande **output**. Une seule valeur de sortie peut être activée à la fois. La valeur par défaut est **output none**. Cette valeur annule toute sortie des commandes **action**. La commande s'exécute en mode de configuration globale en tant qu'utilisateur ayant le niveau de privilège 15 (le plus élevé). La commande ne peut accepter aucune entrée, car elle est désactivée. Vous pouvez envoyer la sortie des commandes **action** de l'interface de ligne de commande à l'un des trois emplacements suivants :

- **None** (Aucun), qui est la valeur par défaut et ignore la sortie.
- **Console**, qui envoie les données de sortie à la console ASA.
- **File** (Fichier), qui envoie la sortie dans un fichier. Les quatre options de fichiers suivantes sont disponibles :
  - **Create a unique file** (Créer un fichier unique), qui crée un nouveau fichier avec un nom unique chaque fois qu'un applet de gestionnaire d'événements est invoqué.
  - **Create/overwrite a file** (Créer/remplacer un fichier), qui remplace un fichier spécifié chaque fois qu'un applet de gestionnaire d'événements est invoqué.

- **Create/append to a file** (Créer/ajouter à un fichier), qui s'ajoute à un fichier spécifié chaque fois qu'un applet de gestionnaire d'événements est invoqué. Si le fichier n'existe pas encore, il est créé.
- **Create a set of files** (Créer un ensemble de fichiers), ce qui crée un ensemble de fichiers portant des noms uniques qui sont tournés chaque fois qu'un applet de gestionnaire d'événements est invoqué.

Lignes directrices pour l'EEG

Cette section décrit les lignes directrices et les limites que vous devez vérifier avant de configurer l'EEG.

Directives relatives au mode contextuel

Non pris en charge en mode de contexte multiple.

Directives supplémentaires

- Lors d'un plantage, l'état de l'ASA est généralement inconnu. Certaines commandes peuvent ne pas être exécutées en toute sécurité dans cette condition.
- Le nom d'un applet de gestionnaire d'événements ne peut pas contenir d'espaces.
- Vous ne pouvez pas modifier les paramètres des événements None (Aucun) et Cashinfo (Renseignements sur le plantage).
- Les performances peuvent être affectées, car les messages du journal système sont envoyés à l'EEG pour traitement.
- La sortie par défaut est **output none** pour chaque applet de gestionnaire d'événements. Pour modifier ce paramètre, vous devez entrer une valeur de sortie différente.
- Vous ne pouvez avoir qu'une seule option de sortie définie pour chaque applet de gestionnaire d'événements.

Configurer l'EEG

La configuration de l'EEG comprend les tâches suivantes :

Procédure

Étape 1 Créer un applet de gestionnaire d'événements et configurer les événements, à la page 1220.
Étape 2 Configurer une action et des destinations pour la sortie d'une action, à la page 1221.
Étape 3 Exécuter un applet de gestionnaire d'événements, à la page 1222.
Étape 4 Suivre l'allocation de mémoire et l'utilisation de la mémoire, à la page 1222.

Créer un applet de gestionnaire d'événements et configurer les événements

Pour créer un applet de gestionnaire d'événements et configurer les événements, procédez comme suit :

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **Embedded Event Manager (Gestionnaire d'événements intégré)**.

Étape 2 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Event Manager Applet** (Ajouter un applet de gestionnaire d'événements).

Étape 3 Saisissez le nom de l'Applet (sans espace) et décrivez ce qu'elle fait. La description peut comporter jusqu'à 256 caractères. Vous pouvez inclure des espaces dans le texte de la description si celui-ci est placé entre guillemets.

Étape 4 Cliquez sur **Add** (Ajouter) dans la zone **Events** (Événements) pour afficher la boîte de dialogue **Add Event Manager Applet Event** (Ajouter un événement d'applet de gestionnaire d'événements).

Étape 5 Choisissez le type d'événement que vous souhaitez configurer dans la liste déroulante **Type**. Les options disponibles sont **crashinfo** (Renseignements de plantage), **None** (Aucun), **Syslog** (Journal système), **Once-a-day timer** (Minuterie une fois par jour), **One-shot timer** (Minuterie unique) et **Periodic timer** (Minuterie périodique).

- **Syslog** (Journal système) : saisissez un seul message de journal système ou une plage de messages de journal système. Si un message de journal système se produit et correspond au message de journal système ou à la plage de messages de journal système spécifié, un applet de gestionnaire d'événements est déclenché. (Facultatif) Saisissez le nombre de fois dans le champ des **occurrences** que le message de journal système doit se produire pour qu'un applet de gestionnaire d'événements soit invoqué. La valeur par défaut est de 1 occurrence toutes les 0 secondes. Les valeurs valides sont comprises entre 1 et 4294967295. (Facultatif) Saisissez le nombre de secondes dans le champ **period** (période) pendant lesquelles les messages de journal système doivent se produire pour invoquer l'action. Cette valeur limite la fréquence d'appel d'un applet de gestionnaire d'événements au maximum une fois dans la période configurée. Les valeurs valides sont comprises entre 0 et 604800. La valeur 0 signifie qu'aucune période n'est définie.
- **Period** (Période) : saisissez la période en secondes. Le nombre de secondes peut aller de 1 à 604800.
- **Once-a-day timer** (Minuterie une fois par jour) : saisissez l'heure du jour au format hh:mm:ss. La plage horaire va de 00:00:00 (minuit) à 23:59:59.
- **One-shot timer** (Minuterie unique) : saisissez la période en secondes. Le nombre de secondes peut aller de 1 à 604800.
- **None** (Aucun) : choisissez cette option pour invoquer manuellement un applet de gestionnaire d'événements.
- **crashinfo** (Renseignements de plantage) : choisissez cette option pour déclencher un événement de plantage lorsque l'ASA tombe en panne.

Configurer une action et des destinations pour la sortie d'une action

Pour configurer une action et des destinations spécifiques pour l'envoi de la sortie d'une action, procédez comme suit :

Procédure

Étape 1 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Event Manager Applet** (Ajouter un applet de gestionnaire d'événements).

Étape 2 Saisissez le nom de l'Applet (sans espace) et décrivez ce qu'elle fait. La description peut comporter jusqu'à 256 caractères.

Étape 3 Cliquez sur **Add** (Ajouter) dans la zone **Actions** pour afficher la boîte de dialogue **Add Event Manager Applet Action** (Ajouter une action d'applet de gestionnaire d'événements).

Étape 4 Saisissez le numéro de séquence unique dans le champ **Sequence #** (N° de séquence). Les numéros de séquence valides sont compris entre 0 et 4294967295.

Étape 5 Saisissez la commande de l'interface de ligne de commande dans le champ **CLI Command** (Commande de l'interface de ligne de commande). La commande s'exécute en mode de configuration globale en tant qu'utilisateur ayant le niveau de privilège 15 (le plus élevé). La commande ne peut accepter aucune entrée, car elle est désactivée.

Étape 6 Cliquez sur **OK** pour fermer la boîte de dialogue **Add Event Manager Applet Action** (Ajouter une action d'applet de gestionnaire d'événements).

L'action nouvellement ajoutée apparaît dans la liste **Actions**.

Étape 7 Cliquez sur **Add** (Ajouter) pour ouvrir la boîte de dialogue **Add Event Manager Applet** (Ajouter un applet de gestionnaire d'événements).

Étape 8 Choisissez l'une des options de destination de sortie disponibles :

- Choisissez l'option **None** (Aucun) dans la liste déroulante **Output Location** (Emplacement de sortie) pour ignorer toute sortie des commandes **action**. Il s'agit du paramètre par défaut.
- Choisissez l'option **Console** dans la liste déroulante **Output Location** (Emplacement de sortie) pour envoyer la sortie des commandes **action** à la console.



Remarque L'exécution de cette commande affecte les performances.

- Choisissez l'option **File** (Fichier) dans la liste déroulante **Output Location** (Emplacement de sortie) pour envoyer la sortie des commandes **action** vers un nouveau fichier pour chaque applet de gestionnaire d'événements invoqué. L'option **Create a unique file** (Créer un fichier unique) est automatiquement sélectionnée par défaut.

  Le nom de fichier a le format eem-*Applet-horodatage.log*, dans lequel *Applet* est le nom de l'Applet du gestionnaire d'événements et *Horodatage* est un horodatage datant au format YYYMMMDD-hhmmss.

- Choisissez l'option **File** (Fichier) dans la liste déroulante **Output Location** (Emplacement de sortie), puis choisissez l'option **Create a set of files** (Créer un ensemble de fichiers) dans la liste déroulante pour créer un ensemble de fichiers rotatifs.

Lorsqu'un nouveau fichier doit être écrit, le fichier le plus ancien est supprimé et tous les fichiers suivants sont renumérotés avant l'écriture du premier fichier. Le fichier le plus récent est indiqué par 0, et le fichier le plus ancien est indiqué par le nombre le plus élevé. Les valeurs valides pour la plage de valeurs de rotation sont comprises entre 2 et 100. Le format du nom de fichier est eem-*Applet*-*x*.log, dans lequel *Applet* est le nom de l'applet et *x* est le numéro de fichier.

- Choisissez l'option **File** (Fichier) dans la liste déroulante **Output Location** (Emplacement de sortie), puis l'option **Create/overwrite a file** (Créer/remplacer un fichier) dans la liste déroulante pour écrire la sortie de la commande **action** dans un fichier unique, qui est remplacé chaque fois.
- Choisissez l'option **File**(Fichier) dans la liste déroulante **Output Location** (Emplacement de sortie), puis l'option **Create/append a file** (Créer/ajouter un fichier) dans la liste déroulante pour écrire la sortie de la commande **action** dans un fichier unique, mais ce fichier est ajouté à chaque fois.

Étape 9 Cliquez sur **OK** pour fermer la boîte de dialogue **Add Event Manager Applet** (Ajouter un applet de gestionnaire d'événements).

La destination de sortie spécifiée apparaît dans le volet **Embedded Event Manager** (Gestionnaire d'événements intégré).

Exécuter un applet de gestionnaire d'événements

Pour exécuter un applet de gestionnaire d'événements, procédez comme suit :

Procédure

Étape 1 Dans le volet **Embedded Event Manager** (Gestionnaire d'événements intégré), sélectionnez un applet de gestionnaire d'événements dans la liste qui a été configurée avec l'événement **None** (Aucun).

Étape 2 Cliquez sur **Run** (Exécuter).

Suivre l'allocation de mémoire et l'utilisation de la mémoire

Pour consigner l'allocation de mémoire et l'utilisation de la mémoire, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **Embedded Event Manager (Gestionnaire d'événements intégré)**.

Étape 2 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Event Manager Applet** (Ajouter un applet de gestionnaire d'événements).

Étape 3 Cliquez à nouveau sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Event Manager Applet Event** (Ajouter un événement d'applet de gestionnaire d'événements).

Étape 4 Choisissez **memory-logging-wrap** dans la liste déroulante.

Étape 5 Cliquez sur **OK** pour l'ajouter à la liste **Events** (Événements).

Étape 6 Cliquez à nouveau sur **OK** pour l'ajouter à la liste **Applets**.

Supervision de l'EEG

Consultez les commandes suivantes pour superviser l'EEG.

- **Monitoring (Supervision) > Properties (Propriétés) > EEM Applets (Applets EEG)**

  Ce volet affiche la liste des applets EEM et leur nombre d'accès.

- **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

Historique de l'EEG

Tableau 59 : Historique de l'EEG

Nom de la caractéristique	Versions de plateforme	Description
Gestionnaire d'événements intégré de Cisco (EEG)	9.2(1)	Le service EEG vous permet de déboguer les problèmes et fournit une journalisation à usage général pour le dépannage. Il y a deux composants : les événements auxquels l'EEG répond ou écoute, et les applets de gestionnaire d'événements qui définissent les actions ainsi que les événements auxquels l'EEG répond. Vous pouvez configurer plusieurs applets de gestionnaire d'événements pour répondre à différents événements et effectuer des actions différentes. Nous avons introduit les écrans suivants : **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Embedded Event Manager (Gestionnaire d'événements intégré), Monitoring (Supervision) > Properties (Propriétés) > EEM Applets (Applets EEG)**.
Suivi de mémoire pour l'EEG	9.4(1)	Nous avons ajouté une nouvelle fonctionnalité de débogage pour consigner les allocations de mémoire et l'utilisation de la mémoire, et pour répondre aux événements d'encapsulation de la journalisation de la mémoire. Nous avons modifié l'écran suivant : **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Embedded Event Manager (Gestionnaire d'événements intégré) > Add Event Manager Applet (Ajouter un applet de gestionnaire d'événements) > Add Event Manager Applet Event (Ajouter un événement d'applet de gestionnaire d'événements)**.



CHAPITRE 47

Tests et dépannage

Ce chapitre décrit comment dépanner l'ASA et tester la connectivité de base.

- Récupérer les mots de passe d'activation et Telnet, à la page 1225
- Configurer et exécuter des captures à l'aide de l'Assistant de capture de paquets, à la page 1229
- Utilisation et rapport d'utilisation du processeur (CPU), à la page 1236
- Tester votre configuration, à la page 1241
- Supervision des performances et des ressources du système, à la page 1250
- Supervision des connexions, à la page 1252
- Historique des tests et du dépannage , à la page 1253

Récupérer les mots de passe d'activation et Telnet

Si vous oubliez les mots de passe d'activation ou Telnet, vous pouvez les récupérer pour les modèles ASA virtuel et ISA 3000. Vous devez effectuer la tâche à l'aide de l'interface de ligne de commande.

Remarque Pour les autres plateformes, vous ne pouvez pas récupérer les mots de passe perdus. Vous pouvez uniquement restaurer la configuration d'usine par défaut et réinitialiser les mots de passe par défaut. Pour Firepower 4100/9300, consultez le Guide de configuration de FXOS. Pour les autres modèles, consultez le Guide de dépannage de FXOS.

Récupérer les mots de passe sur l'ISA 3000

Pour récupérer les mots de passe des ISA 3000, procédez comme suit :

Procédure

Étape 1 Connectez-vous au port de console de l'ASA.

Étape 2 Mettez l'ASA hors tension, puis rallumez-le.

Étape 3 Après le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à passer en mode ROMMON.

Étape 4 Pour mettre à jour la valeur du registre de configuration, entrez la commande suivante :

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

L'ASA affiche la valeur actuelle du registre de configuration et une liste d'options de configuration. Enregistrez la valeur actuelle du registre de configuration afin de pouvoir la restaurer ultérieurement.

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ...... auto-boot index 1 image in disks
```

Étape 5 Rechargez l'ASA en saisissant la commande suivante :

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

L'ASA charge la configuration par défaut au lieu de la configuration de démarrage.

Étape 6 Accédez au mode d'exécution privilégié en saisissant la commande suivante :

```
ciscoasa# enable
```

Étape 7 Lorsque le mot de passe vous est demandé, appuyez sur **Entrée**.

Le mot de passe est une valeur vide.

Étape 8 Chargez la configuration de démarrage en saisissant la commande suivante :

```
ciscoasa# copy startup-config running-config
```

Étape 9 Accédez au mode de configuration globale en saisissant la commande suivante :

```
ciscoasa# configure terminal
```

Étape 10 Modifiez les mots de passe, au besoin, dans la configuration par défaut en saisissant les commandes suivantes :

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

Étape 11 Chargez la configuration par défaut en saisissant la commande suivante :

```
ciscoasa(config)# no config-register
```

La valeur par défaut du registre de configuration est 0x1. Voir la référence des commandes pour en savoir plus sur le registre de configuration.

Étape 12 Enregistrez les nouveaux mots de passe dans la configuration de démarrage en saisissant la commande suivante :

```
ciscoasa(config)# copy running-config startup-config
```

Récupérer les mots de passe ou les images sur l'ASA virtuel

Pour récupérer les mots de passe ou les images sur l'ASA virtuel, procédez comme suit :

Procédure

Étape 1 Copiez la configuration en cours d'exécution dans un fichier de sauvegarde sur l'ASA virtuel :

copy running-config *nom de fichier*

Exemple :

```
ciscoasa# copy running-config backup.cfg
```

Étape 2 Redémarrez l'ASA virtuel :

reload

Étape 3 Dans le menu GNU GRUB, appuyez sur la flèche vers le bas, choisissez <**filename**> **sans option de chargement de configuration**, puis appuyez sur **Enter** (Entrée). Le nom de fichier est le nom de fichier d'image de démarrage par défaut sur l'ASA virtuel. L'image de démarrage par défaut n'est jamais démarrée automatiquement par la commande **fallback**. Chargez ensuite l'image de démarrage sélectionnée.

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

Exemple :

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

Étape 4 Copiez le fichier de configuration de sauvegarde vers la configuration en cours d'exécution.

copy *nom_de_fichier* **running-config**

Exemple :

```
ciscoasa (config)# copy backup.cfg running-config
```

Étape 5 Réinitialisez le mot de passe.

enable password *password*

Exemple :

```
ciscoasa(config)# enable password cisco123
```

Étape 6 Enregistrez la nouvelle configuration.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Désactiver la récupération du mot de passe pour le matériel ISA 3000



Remarque Vous ne pouvez pas désactiver la récupération du mot de passe sur les modèles ASA virtuel, Secure Firewall.

Pour désactiver la récupération du mot de passe et vous assurer que les utilisateurs non autorisés ne peuvent pas utiliser le mécanisme de récupération du mot de passe pour compromettre l'ASA, procédez comme suit.

Avant de commencer

Sur l'ASA, la commande **no service password-recovery** vous empêche de passer en mode ROMMON avec la configuration intacte. Lorsque vous passez en mode ROMMON, l'ASA vous invite à effacer tous les systèmes de fichiers flash. Vous ne pouvez pas passer en mode ROMMON sans effectuer au préalable cet effacement. Si vous choisissez de ne pas effacer le système de fichiers flash, l'ASA se recharge. Étant donné que la récupération du mot de passe dépend de l'utilisation du mode ROMMON et du maintien de la configuration existante, cet effacement vous empêche de récupérer un mot de passe. Cependant, la désactivation de la récupération du mot de passe empêche les utilisateurs non autorisés d'afficher la configuration ou d'insérer des mots de passe différents. Dans ce cas, pour restaurer le système à un état de fonctionnement, chargez une nouvelle image et un fichier de configuration de sauvegarde, le cas échéant.

La commande **service password-recovery** apparaît dans le fichier de configuration pour information uniquement. Lorsque vous saisissez la commande à l'invite de l'interface de ligne de commande, le paramètre est enregistré dans la NVRAM. La seule façon de modifier le paramètre est d'entrer la commande à l'invite de l'interface de ligne de commande. Le chargement d'une nouvelle configuration avec une version différente de la commande ne modifie pas le paramètre. Si vous désactivez la récupération du mot de passe lorsque l'ASA est configuré pour ignorer la configuration de démarrage au démarrage (en préparation de la récupération du mot de passe), l'ASA modifie le paramètre pour charger la configuration de démarrage comme d'habitude. Si vous utilisez le basculement et que l'unité de secours est configurée pour ignorer la configuration de

démarrage, la même modification est apportée au registre de configuration lorsque la commande **no service password- recovery** est dupliquée sur l'unité de secours.

Procédure

Désactivez la récupération du mot de passe.

no service password-recovery

Exemple :

```
ciscoasa (config)# no service password-recovery
```

Configurer et exécuter des captures à l'aide de l'Assistant de capture de paquets

Vous pouvez utiliser l'assistant de capture de paquets pour configurer et exécuter des captures pour le dépannage des erreurs. Les captures peuvent utiliser des ACL pour limiter le type de trafic capturé, les adresses et les ports source et de destination, et une ou plusieurs interfaces. L'assistant exécute une capture sur chacune des interfaces d'entrée et de sortie. Vous pouvez enregistrer les captures sur votre PC pour les examiner dans un analyseur de paquets.

Remarque Cet outil ne prend pas en charge la capture de SSL VPN sans client.

Pour configurer et exécuter des captures, procédez comme suit.

Procédure

Étape 1 Choisissez **Wizards (Assistants)** > **Packet Capture Wizard (Assistant de capture de paquets)**.

L'écran **Overview of Packet Capture** (Aperçu de la capture de paquets) apparaît, avec une liste des tâches que l'assistant vous guidera pour accomplir. Ces tâches comprennent les éléments suivants :

- Sélection d'une interface d'entrée.
- Sélection d'une interface de sortie.
- Définition des paramètres du tampon.
- Exécution des captures.
- Enregistrement des captures sur votre PC (facultatif).

Étape 2 Cliquez sur **Next** (suivant).

Dans un environnement de grappe, l'écran **Cluster Option** (Option de grappe) s'affiche. Passez à l'étape 3.

Dans un environnement sans grappe, l'écran **Ingress Traffic Selector** (Sélecteur de trafic d'entrée) s'affiche. Passez à l'étape 4.

Étape 3 Choisissez l'une des options suivantes dans l'écran **Cluster Option** (Pption de grappe) pour exécuter une capture : **This device only** (Ce périphérique uniquement) ou **The whole cluster** (L'ensemble de la grappe), puis cliquez sur **Next** (Suivant) pour afficher l'écran **Ingress Selector** (Sélecteur d'entrée).

Étape 4 Cliquez sur le bouton radio **Select Interface** (Sélectionner l'interface) pour capturer des paquets sur une interface.

Dans un environnement de mise en grappe, pour capturer uniquement les paquets du plan de commande de grappe, cochez la case **CP-Cluster** (Grappe CP).

Étape 5 Cliquez sur le bouton radio **Use backplane channel** (Utiliser le canal de fond de panier) pour capturer des paquets dans le plan de données ASA CX.

Étape 6 Effectuez l'une des opérations suivantes dans la zone **Packet Match Criteria** (Critères de correspondance des paquets) :

- Cliquez sur le bouton radio **Select access list (Sélectionner la liste d'accès)** pour spécifier l'ACL à utiliser pour les paquets correspondants, puis choisissez l'ACL dans la liste déroulante **Select ACL** (Sélectionner une ACL). Cliquez sur **Manage** (Gérer) pour afficher le volet **ACL Manager** (Gestionnaire ACL) afin d'ajouter une ACL précédemment configurée à la liste déroulante actuelle. Choisissez une ACL, puis cliquez sur **OK**.

  L'option de liste d'accès est désactivée lorsque vous activez la capture de paquet de commutateurs. Pour de plus amples renseignements, consultez la section Sélecteur de trafic d'entrée, à la page 1233.

- Cliquez sur le bouton radio **Specify Packet Parameters** pour spécifier les paramètres des paquets.

a) Effectuez l'une des opérations suivantes dans la liste déroulante **ICMP Capture** (Capture ICMP) :

Remarque Le champ **ICMP Capture** (Capture ICMP) est rempli uniquement lorsque vous sélectionnez **The whole cluster** (L'ensemble de la grappe) comme option de grappe dans la fenêtre précédente.

- Sélectionnez **include-decrypted** pour capturer les paquets IPsec déchiffrés qui contiennent du trafic normal et déchiffré une fois qu'ils pénètrent dans le périphérique de pare-feu.
- Sélectionnez **persist** pour capturer les paquets persistants sur les unités de grappe.

Étape 7 Pour continuer, consultez Sélecteur de trafic d'entrée, à la page 1233.

Étape 8 Cliquez sur **Next** (Suivant) pour afficher l'écran **Egress Traffic Selector** (Sélecteur de trafic de sortie).

Étape 9 Cliquez sur le bouton radio **Select Interface** (Sélectionner l'interface) pour capturer des paquets sur une interface.

Dans un environnement de mise en grappe, pour capturer les paquets du plan de commande de grappe, cochez la case **CP-Cluster** (Grappe CP).

Remarque Pour en savoir plus sur les champs Egress Traffic Selector (Sélecteur de trafic de sortie), consultez Sélecteur de trafic de sortie, à la page 1234.

Pour en savoir plus sur les champs Egress Traffic Selector (Sélecteur de trafic de sortie), consultez Sélecteur de trafic de sortie, à la page 1234.

Étape 10 Cliquez sur **Next** (Suivant) pour afficher l'écran **Buffers & Captures** (Tampons et captures). Pour continuer, consultez Buffers (Tampons).

Étape 11 Cochez la case **Get capture every 10 seconds** (Obtenir une capture toutes les 10 secondes) dans la zone **Capture Parameters** (Paramètres de capture) pour obtenir automatiquement la dernière capture toutes les 10 secondes. Par défaut, cette capture utilise le tampon circulaire.

Étape 12 Vous spécifiez la taille du tampon et la taille des paquets dans la zone **Buffer Parameters** (Paramètres du tampon). La taille de tampon est la quantité maximale de mémoire que la capture peut utiliser pour stocker les paquets. La taille de paquet est le paquet le plus long que la capture peut contenir. Nous vous conseillons d'utiliser la taille de paquet la plus longue pour capturer le plus de renseignements possible.

a) (Facultatif. Applicable uniquement aux périphériques Secure Firewall 3100) Cochez la case **Switch** (Commutateur) pour stocker les paquets de commutation capturés.
b) Saisissez la taille de paquet. La taille valide varie de 14 à 1522 octets. Pour la capture de paquets de commutateurs, la taille valide varie de 64 à 9006 octets.
c) Saisissez la taille de tampon. La taille valide varie de 1534 et 33554432 octets. Pour la capture de paquets de commutateurs, la taille valide varie de 256 à 2048 octets.
d) Cochez la case **Use circular buffer** (Utiliser le tampon circulaire) pour stocker les paquets capturés.

Remarque Lorsque vous choisissez ce paramètre, si toute la mémoire tampon est utilisée, la capture commence à remplacer les paquets les plus anciens.

Étape 13 Cliquez sur **Next** (Suivant) pour afficher l'écran **Summary** (Résumé), qui affiche les options de grappe pour toutes les unités de la grappe (si vous utilisez la mise en grappe), les sélecteurs de trafic et les paramètres de tampon que vous avez saisis. Pour continuer, consultez Summary (Résumé).

Étape 14 Cliquez sur **Next** (Suivant) pour afficher l'écran **Run Captures** (Exécuter les captures), puis sur **Start** (Démarrer) pour commencer à capturer les paquets. Cliquez sur **Stop** (Arrêter) pour mettre fin à la capture. Pour continuer, consultez Exécuter des captures, à la page 1235. Si vous utilisez la mise en grappe, passez à l'étape 16.

Étape 15 Cliquez sur **Get Capture Buffer** (Obtenir le tampon de capture) pour déterminer l'espace tampon restant. Cliquez sur **Clear Buffer on Device** (Effacer le tampon de l'appareil) pour supprimer le contenu actuel et faire de la place dans le tampon pour capturer plus de paquets.

Étape 16 Dans un environnement de mise en grappe, sur l'écran **Run Captures** (Exécuter les captures), effectuez une ou plusieurs des étapes suivantes :

- Cliquez sur **Get Cluster Capture Summary** (Obtenir le résumé de la capture de la grappe) pour afficher un résumé des renseignements sur la capture de paquets pour toutes les unités de la grappe, suivis des renseignements sur la capture de paquets pour chaque unité.

- Cliquez sur **Get Capture Buffer** (Obtenir le tampon de capture) pour déterminer l'espace tampon restant dans chaque unité de la grappe. La boîte de dialogue **Capture Buffer from Device** (Capturer le tampon de l'appareil) s'affiche.
- Cliquez sur **Clear Capture Buffer** (Effacer le tampon de capture) pour supprimer le contenu actuel d'une ou de toutes les unités d'une grappe et faire de la place dans le tampon pour capturer plus de paquets.

Étape 17 Cliquez sur **Save captures** (Enregistrer les captures) pour afficher la boîte de dialogue **Save Capture** (Enregistrer la capture). Vous avez la possibilité d'enregistrer la capture d'entrée, la capture de sortie ou les deux. Pour continuer, consultez Save Captures (Enregistrer les captures).

Étape 18 Cliquez sur **Save Ingress Capture** (Enregistrer la capture d'entrée) pour afficher la boîte de dialogue **Save capture file** (Enregistrer le fichier de capture). Spécifiez l'emplacement de stockage sur votre PC, puis cliquez sur **Save** (Enregistrer).

Étape 19 Cliquez sur **Launch Network Sniffer Application** (Lancer l'application de l'analyseur de réseau) pour démarrer l'application d'analyse de paquet spécifiée dans **Tools (Outils)** > **Preferences (Préférences)** pour l'analyse de la capture d'entrée.

Étape 20 Cliquez sur **Save Egress Capture** (Enregistrer la capture de sortie) pour afficher la boîte de dialogue **Save capture file** (Enregistrer le fichier de capture). Spécifiez l'emplacement de stockage sur votre PC, puis cliquez sur **Save** (Enregistrer).

Étape 21 Cliquez sur **Launch Network Sniffer Application** (Lancer l'application de l'analyseur de réseau) pour démarrer l'application d'analyse de paquet spécifiée dans **Tools (Outils)** > **Preferences (Préférences)** pour l'analyse de la capture de sortie.

Étape 22 Cliquez sur **Close** (Fermer), puis **Finish** (Terminer) pour quitter l'assistant.

Lignes directrices pour la capture des paquets

Mode contextuel

- Vous pouvez configurer les captures sur la liaison de commande de grappe dans un contexte; seul le paquet associé au contexte envoyé dans la liaison de commande de grappe est capturé.
- Vous ne pouvez configurer qu'une seule capture pour un VLAN partagé; si vous configurez une capture dans plusieurs contextes sur le VLAN partagé, seule la dernière capture configurée est utilisée.
- Si vous supprimez la dernière capture configurée (active), aucune capture ne devient active, même si vous avez déjà configuré une capture dans un autre contexte; vous devez supprimer la capture et l'ajouter à nouveau pour la rendre active.
- Tout le trafic qui entre dans l'interface à laquelle la capture est connectée est capturé, y compris le trafic vers d'autres contextes sur le VLAN partagé. Par conséquent, si vous activez une capture dans le contexte A pour un VLAN qui est également utilisé par le contexte B, le trafic entrant du contexte A et du contexte B est capturé.
- Pour le trafic de sortie, seul le trafic du contexte avec la capture active est capturé. La seule exception est lorsque vous n'activez pas l'inspection ICMP (par conséquent, le trafic ICMP n'a pas de session dans le chemin accéléré). Dans ce cas, le trafic ICMP d'entrée et de sortie pour tous les contextes sur le VLAN partagé est capturé.

Directives supplémentaires

- Si l'ASA reçoit des paquets avec un en-tête TCP mal formaté et les abandonne du fait de la raison d'abandon ASP *invalid-tcp-hdr-length*, la sortie de la commande **show capture** sur l'interface où ces paquets sont reçus n'affiche pas ces paquets.
- Vous pouvez uniquement capturer le trafic IP; vous ne pouvez pas capturer des paquets non IP tels que les ARP.
- Pour les paquets marqués SGT en ligne, les paquets capturés contiennent un en-tête CMD supplémentaire que votre visualiseur PCAP pourrait ne pas comprendre.
- Les captures de paquets comprennent les paquets que le système modifie ou injecte dans la connexion en raison de l'inspection, de la normalisation de la NAT, du TCP ou d'autres fonctionnalités qui ajustent le contenu d'un paquet.
- La trace de la durée de vie d'un paquet virtuel injecté dans un chemin de données ne reflète pas exactement la façon dont le chemin de données gère les paquets physiques. Cette différence dépend de la version du logiciel, de la configuration et du type de paquets virtuels injectés. Voici les paramètres de configuration qui pourraient entraîner cette disparité :
  - Il existe au moins 2 instructions NAT pour le même hôte.
  - Les flux avant et arrière d'une connexion ont des protocoles différents. Par exemple, le flux avant est UDP ou TCP, le flux arrière est ICMP.
  - L'inspection d'erreurs ICMP est activée.

Sélecteur de trafic d'entrée

Pour configurer l'interface d'entrée, les hôtes ou réseaux source et de destination, ainsi que le protocole de capture de paquets, procédez comme suit :

Procédure

Étape 1 Choisissez le nom de l'interface d'entrée dans la liste déroulante.

Étape 2 Saisissez l'hôte et le réseau de la source d'entrée. Cliquez sur le bouton radio **Use backplane channel** (Utiliser le canal de fond de panier) pour capturer des paquets dans le plan de données ASA CX.

Étape 3 Saisissez l'hôte et le réseau de destination d'entrée.

Étape 4 Saisissez le type de protocole à capturer. Les protocoles disponibles sont ah, eigrp, esp, gre, icmp, icmp6, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, snp, tcp ou udp.

a) Saisissez le type ICMP pour ICMP uniquement. Les types disponibles sont les suivants : all, alternate address, conversion-error, echo, echo-reply, information-reply, information-request, mask-reply, mask-request, mobile-redirect, parameter-problem, redirect, router-advertisement, router-solicitation, source-quench, time-exceeded, timestamp-reply, timestamp-request, traceroute ou unreachable.

b) Spécifiez les services de port source et destination pour les protocoles TCP et UDP uniquement. Les options disponibles sont les suivantes :
   - Choisissez **All Services** (Tous les services) pour inclure tous les services.
   - Choisissez **Service Groups** (Groupes de services) pour inclure un groupe de service.

Pour inclure un service spécifique, choisissez l'une des options suivantes : aol, bgp, chargen, cifx, citrix-ica, ctiqbe, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, https, ident, imap4, irc, kerberos, klogin, kshell, ldap, ldaps, login, lotusnotes, lpd, netbios-ssn, nntp, pcanywhere-data, pim-auto-rp, pop2, pop3, pptp, rsh, rtsp, sip, smtp, sqlnet, ssh, sunrpc, tacacs, talk, telnet, uucp, or whois.

Étape 5 Pour activer la capture de paquets pour le service Cisco TrustSec, dans la zone **Security Group Tagging** (Balisation du groupe de sécurité), cochez la case **SGT number** (Numéro SGT) et saisissez le numéro de balise du groupe de sécurité. Les numéros de balise de groupe de sécurité valides sont compris entre 2 et 65519.

Étape 6 (Facultatif. Applicable uniquement aux périphériques Secure Firewall 3100) Pour activer la capture de paquets du commutateur, dans la zone **Switch Control** (Contrôle du commutateur), cochez la case **Switch** (Commutateur) et spécifiez les plages de VLAN interne et de VLAN externe (de 1 à 4096).

Remarque Lorsque vous activez la capture de paquets de commutateurs, l'option de liste d'accès est désactivée.

Sélecteur de trafic de sortie

Pour configurer l'interface de sortie, les hôtes/réseaux source et de destination, ainsi que les services de port source et de destination pour la capture de paquets, procédez comme suit :

Procédure

Étape 1 Cliquez sur le bouton radio **Select Interface** (Sélectionner l'interface) pour capturer des paquets sur une interface. Cliquez sur le bouton radio **Use backplane channel** (Utiliser le canal de fond de panier) pour capturer des paquets dans le plan de données ASA CX.

Étape 2 Choisissez le nom de l'interface de sortie dans la liste déroulante.

Étape 3 Saisissez l'hôte et le réseau source de sortie.

Étape 4 Saisissez l'hôte et le réseau de destination de sortie.

Le type de protocole sélectionné lors de la configuration d'entrée est déjà répertorié.

Étape 5 (Facultatif. Applicable uniquement aux périphériques Secure Firewall 3100) Si vous avez activé la capture de paquets du commutateur, précisez les plages de VLAN interne et de VLAN externe (de 1 à 4096). Pour activer la capture de paquets du commutateur, consultez Sélecteur de trafic d'entrée, à la page 1233.

Tampons

Pour configurer la taille des paquets, la taille du tampon et l'utilisation du tampon circulaire pour la capture de paquets, procédez comme suit :

Procédure

Étape 1 Saisissez le paquet le plus long que la capture peut contenir. Utilisez la plus longue taille disponible pour capturer le plus de renseignements possible.

Étape 2 Saisissez la quantité maximale de mémoire que la capture peut utiliser pour stocker les paquets.

Étape 3 Utilisez le tampon circulaire pour stocker les paquets. Lorsque le tampon circulaire a utilisé toute la mémoire tampon, la capture écrase d'abord les paquets les plus anciens.

Résumé

L'écran **Summary** (Résumé) affiche les options de grappe (si vous utilisez la mise en grappe), les sélecteurs de trafic et les paramètres de tampon pour la capture de paquets sélectionnée dans les écrans précédents de l'assistant.

Exécuter des captures

Pour démarrer et arrêter la session de capture, afficher le tampon de capture, lancer une application d'analyse de réseau, enregistrer les captures de paquets et effacer le tampon, procédez comme suit :

Procédure

Étape 1 Cliquez sur **Start** (Démarrer) pour commencer la session de capture de paquets sur une interface sélectionnée.

Étape 2 Cliquez sur **Stop** (Arrêter) pour arrêter la session de capture de paquets sur une interface sélectionnée.

Étape 3 Cliquez sur **Get Capture Buffer** (Obtenir le tampon de capture) pour obtenir un instantané des paquets capturés sur l'interface.

Étape 4 Cliquez sur **Ingress** (Entrée) pour afficher le tampon de capture sur l'interface d'entrée.

Étape 5 Cliquez sur **Egress** (Sortie) pour afficher le tampon de capture sur l'interface de sortie.

Étape 6 Cliquez sur **Clear Buffer on Device** (Effacer le tampon sur le périphérique) pour effacer le tampon du périphérique.

Étape 7 Cliquez sur **Launch Network Sniffer Application** (Lancer l'application de l'analyseur de réseau) pour démarrer l'application d'analyse de paquet afin d'analyser la capture d'entrée ou la capture de sortie spécifiée dans **Tools (Outils)** > **Preferences (Préférences)**.

Étape 8 Cliquez sur **Save Captures** (Enregistrer les captures) pour enregistrer les captures d'entrée et de sortie au format ASCII ou PCAP.

Enregistrer des captures

Pour enregistrer les captures de paquets d'entrée et de sortie dans le format de fichier ASCII ou PCAP pour une analyse plus approfondie des paquets, procédez comme suit :

Procédure

Étape 1 Cliquez sur **ASCII** pour enregistrer le tampon de capture au format ASCII.

Étape 2 Cliquez sur **PCAP** pour enregistrer le tampon de capture au format PCAP.

Étape 3 Cliquez sur **Save ingress capture** (Enregistrer la capture d'entrée) pour spécifier un fichier dans lequel enregistrer la capture de paquets d'entrée.

Étape 4 Cliquez sur **Save egress capture** (Enregistrer la capture de sortie) pour spécifier un fichier dans lequel enregistrer la capture de paquets de sortie.

Utilisation et rapport d'utilisation du processeur (CPU)

Le rapport d'utilisation du processeur résume le pourcentage du processeur utilisé pendant la période précisée. En règle générale, le cœur fonctionne à environ 30 à 40 % de la capacité totale du processeur en dehors des heures de pointe et à environ 60 à 70 % de capacité pendant les heures de pointe.

Utilisation de vCPU dans l'ASA virtuel

Utilisez la commande **show cpu usage** sur l'ASA virtuel pour afficher les statistiques d'utilisation du processeur. L'utilisation de vCPU dans ASA virtuel affiche la quantité de vCPU utilisée pour le chemin de données, le point de contrôle et les processus externes.

L'utilisation de vCPU signalée par le fournisseur de services en nuage (comme VMware, Azure, OCI, etc.) comprend l'utilisation de l'ASA virtuel comme décrit plus :

- Temps d'inactivité d'ASA virtuel
- %SYS surdébit utilisé pour la VM ASA virtuel
- Surdébit du déplacement des paquets entre les vSwitches, les vNIC et les pNIC. Ce surdébit peut être assez important.

Exemple d'utilisation du processeur

Voici un exemple dans lequel l'utilisation de vCPU signalée est sensiblement différente :

- Rapports ASA virtuel : 40 %
- DP : 35 %
- Processus externes : 5 %
- Rapports vSphere : 95 %
- ASA (comme les rapports ASA virtuel) : 40 %
- Interrogation ASA inactive : 10 %
- Frais généraux : 45 %

Le surdébit est utilisé pour effectuer des fonctions d'hyperviseur et pour déplacer des paquets entre les NIC et les vNIC à l'aide du vSwitch.

L'utilisation peut dépasser 100 %, car le serveur ESXi peut utiliser des ressources de traitement supplémentaires pour le surdébit au nom de l'ASA virtuel.

Rapport d'utilisation du CPU VMware

Dans vSphere, cliquez sur l'onglet **VM Performance** (Performances de la VM), puis sur **Advanced** (Avancé) pour afficher la liste déroulante **Chart Options** (Options du graphique), qui indique l'utilisation de vCPU pour chaque état (%Utilisateur, %Inactif, %Sys, etc.) de la VM. Ces renseignements sont utiles pour comprendre le point de vue de VMware sur l'utilisation des ressources de CPU.

Sur l'interface shell du serveur ESXi (vous accédez à l'interface shell en utilisant SSH pour vous connecter à l'hôte), esxtop est disponible. Esxtop a une apparence similaire à la commande **top** de Linux et fournit des renseignements sur l'état de la VM pour les performances de vSphere, notamment les suivantes :

- Détails sur l'utilisation du vCPU, de la mémoire et du réseau
- Utilisation du vCPU pour chaque état de chaque VM.
- Mémoire (type M pendant l'exécution) et réseau (type N pendant l'exécution), ainsi que les statistiques et le nombre d'abandons RX

ASA virtuel et graphiques vCenter

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et vCenter :

- Les numéros de graphique vCenter sont toujours supérieurs aux numéros d'ASA virtuel.
- vCenter l'appelle « %CPU usage » (% d'usage du CPU); l'ASA virtuel l'appelle « %CPU utilization » (% d'utilisation du CPU).

Les termes « %CPU utilization » et « %CPU usage » ont des significations différentes :

- CPU utilization fournit des statistiques sur les CPU physiques.
- CPU usage fournit des statistiques sur les CPU logiques, qui sont basées sur l'hyperthreading du processeur. Mais, comme un seul vCPU est utilisé, l'hyperthreading n'est pas activé.

vCenter calcule le pourcentage d'usage du CPU comme suit :

Nombre de processeur (CPU) virtuels utilisés activement, spécifié en pourcentage du nombre total de CPU disponibles

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'usage du CPU virtuel est l'usage en MHz/nombre de CPU virtuels x fréquence du cœur.

Lorsque vous comparez l'utilisation en MHz, les chiffres de vCenter et d'ASA virtuel correspondent. Selon le graphique vCenter, l'utilisation du CPU en % MHz est calculée comme suit : 60/(2499 x 1 vCPU) = 2,4

Rapports d'utilisation du CPU Amazon CloudWatch

Vous pouvez afficher l'explorateur de mesures pour surveiller les ressources en fonction de leurs balises et de leurs propriétés. Procédez comme suit pour afficher les statistiques d'utilisation du processeur pour une instance en particulier :

Procédure

Étape 1 Ouvrez la console **CloudWatch** et choisissez **Metrics** (Mesures) dans le volet de navigation.

Étape 2 Sélectionnez l'espace de noms de la mesure **EC2** et sélectionnez la dimension **Per-instance Metrics** (Mesures par instance).

Étape 3 Saisissez **CPU Utilization** (Utilisation du CPU) dans le champ de recherche et appuyez sur Entrée. Sélectionnez la ligne de l'instance requise pour afficher un graphique de la mesure **CPU Utilization** (Utilisation du CPU) pour cette instance.

Pour en savoir plus, consultez la documentation relative à Amazon CloudWatch.

ASA virtuel et graphiques Amazon CloudWatch

Les chiffres du graphique Amazon CloudWatch sont supérieurs aux chiffres réels en raison des différentes façons de calculer l'utilisation du CPU sur l'ASA virtuel et le CloudWatch.

Lorsque l'ASA virtuel fonctionne en mode d'interrogation, chaque CPU exécute une boucle de commandes allégées au lieu d'entrer en mode d'économie d'alimentation ou dans tout autre état inactif. Cela améliore les performances en maintenant chaque cœur actif en tout temps au lieu de devoir l'activer/le désactiver ou que leurs horloges soient ajustées en fonction des états d'alimentation Intel.

À l'intérieur de l'ASA virtuel, cette activité est comprise comme un comportement inactif et l'utilisation du CPU est correctement calculée. Cependant, sur Amazon CloudWatch, le comportement inactif ressemble à une activité normale du CPU, car tous les cycles du CPU ont des instructions à exécuter, ce qui conduit le CloudWatch à afficher un pourcentage d'utilisation du CPU élevé (85 à 90 %).

Rapport d'utilisation du CPU Azure

Effectuez les étapes suivantes pour afficher le % d'utilisation du CPU sur toutes les VM surveillées à l'aide des observations de VM du moniteur Azure :

Procédure

Étape 1 Accédez au portail Azure, sélectionnez **Monitor** (Superviser) et choisissez **Virtual Machines** (Machines virtuelles) dans la section **Solutions**.

Étape 2 Sélectionnez l'onglet **Performance** pour afficher le tableau **CPU Utilization %** (% d'utilisation du CPU). Ce tableau affiche les cinq machines ayant la plus forte utilisation moyenne du processeur.

Effectuez les étapes suivantes pour afficher le tableau du % d'utilisation du CPU directement à partir d'une machine virtuelle Azure spécifique :

Procédure

Étape 1 Accédez au portail Azure et sélectionnez **Virtual Machines** (Machines virtuelles).

Étape 2 Dans la liste des VM, choisissez une VM.

Étape 3 Dans la section **Monitoring** (Supervision), sélectionnez **Insights** (Observations).

Étape 4 Sélectionnez l'onglet **Performance**.

Consultez la section Comment représenter graphiquement les performances avec les observations de VM pour en savoir plus.

Graphiques ASA virtuel et Azure

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et Azure. Les numéros du graphique Azure sont toujours supérieurs aux numéros de l'ASA virtuel, car Azure calcule l'utilisation en % du CPU comme la quantité de CPU virtuels utilisés activement, spécifié en pourcentage du total des CPU disponibles.

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'utilisation du CPU virtuel est l'utilisation en MHz/nombre de CPU virtuels x fréquence du cœur.

Azure limite également la quantité de CPU demandée par le système d'exploitation invité. Imaginez un scénario dans lequel l'ASA virtuel signale une utilisation du CPU à 40 % et l'hyperviseur signale une utilisation du CPU à 90 %. Maintenant, si l'ASA virtuel a besoin de plus de puissance de traitement, l'utilisation du CPU peut dépasser 80 % et l'hyperviseur peut alors signaler l'utilisation du CPU à plus de 95 %. Cela conduit l'hyperviseur à limiter le CPU de l'ASA virtuel même si l'ASA virtuel n'exécute qu'une boucle de commandes légères en mode d'interrogation et présente un comportement inactif.

Rapport d'utilisation du CPU Hyper-V

En plus d'afficher les renseignements de configuration du CPU, de la RAM et de l'espace disque pour les serveurs en nuage disponibles, vous pouvez également afficher les renseignements sur le disque, les E/S et le réseau. Utilisez ces renseignements pour vous aider à décider quel serveur en nuage correspond à vos besoins. Vous pouvez afficher les serveurs disponibles par le biais du client nova de ligne de commande ou de l'interface du **panneau de commande en nuage**.

Dans la ligne de commande, exécutez la commande suivante :

```
nova flavor-list
```

Toutes les configurations de serveur disponibles sont affichées. La liste contient les renseignements suivants :

- ID – ID de configuration du serveur
- Name – nom de la configuration, étiqueté par taille de RAM et type de performance

- Mémoire_Mo – la quantité de RAM pour la configuration
- Disque – la taille du disque en Go (pour les serveurs en nuage à usage général, la taille du disque système)
- Éphémère – la taille du disque de données
- Permutation – la taille de l'espace de permutation
- VCPU – le nombre de CPU virtuels associés à la configuration
- Facteur_RXTX – la quantité de bande passante, en Mbit/s, allouée aux ports PublicNet, aux ports ServiceNet et aux réseaux isolés (réseaux en nuage) reliés à un serveur.
- Est_Public – non utilisé

Graphiques ASA virtuel et Hyper-V

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et Hyper-V :

- Les numéros de graphique Hyper-V sont toujours supérieurs aux numéros d'ASA virtuel.
- Hyper-V l'appelle « %CPU usage » (% d'usage du CPU); l'ASA virtuel l'appelle « %CPU utilization » (% d'utilisation du CPU).

Les termes « %CPU utilization » et « %CPU usage » ont des significations différentes :

- CPU utilization fournit des statistiques sur les CPU physiques.
- CPU usage fournit des statistiques sur les CPU logiques, qui sont basées sur l'hyperthreading du processeur. Mais, comme un seul vCPU est utilisé, l'hyperthreading n'est pas activé.

Hyper-V calcule le pourcentage d'usage du CPU comme suit :

Nombre de processeur (CPU) virtuels utilisés activement, spécifié en pourcentage du nombre total de CPU disponibles

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'usage du CPU virtuel est l'usage en MHz/nombre de CPU virtuels x fréquence du cœur.



Remarque Il est conseillé de consulter les rapports d'ASA virtuel pour obtenir un pourcentage d'usage précis du processeur.

Rapport d'utilisation du CPU OCI

Vous pouvez afficher le % d'utilisation du processeur dans le protocole OCI à l'aide de la mesure d'instance de calcul : **oci_computeagent**. La mesure d'utilisation du CPU affiche le niveau d'activité du CPU et est exprimée en pourcentage de temps total. Effectuez les étapes suivantes pour afficher les tableaux de mesures pour une seule instance de calcul :

Procédure

Étape 1 Ouvrez le menu de navigation et cliquez sur **Instances** sous **Compute** (Calcul).

Étape 2 Cliquez sur une instance, puis sur **Metrics** (Mesures) sous **Resources** (Ressources).

Étape 3 Sélectionnez **oci_computeagent** dans la liste Metric namespace (Espace de noms de mesures).

Consultez la section Mesures des instances de calcul pour en savoir plus.

ASA virtuel et graphiques OCI

Les numéros du graphique OCI sont toujours supérieurs aux numéros de l'ASA virtuel, car l'OCI calcule l'utilisation en % du CPU comme la quantité de CPU virtuels utilisés activement, spécifié en pourcentage du total des CPU disponibles.

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'utilisation du CPU virtuel est l'utilisation en MHz/nombre de CPU virtuels x fréquence du cœur.

Tester votre configuration

Cette section décrit comment tester la connectivité pour l'ASA en mode unique ou pour chaque contexte de sécurité, comment envoyer un message Ping aux interfaces ASA et comment autoriser les hôtes d'une interface à envoyer un message Ping aux hôtes sur une autre interface.

Tester la connectivité de base : envoi d'un ping à des adresses

Ping est une commande simple qui vous permet de déterminer si une adresse particulière est active et réactive. Les rubriques suivantes fournissent des renseignements supplémentaires sur la commande et les types de tests que vous pouvez effectuer avec celle-ci.

Ce que vous pouvez tester en utilisant le ping

Lorsque vous envoyez un message Ping à un périphérique, un paquet est envoyé à ce dernier, qui renvoie une réponse. Ce processus permet aux périphériques réseau de se détecter, de s'identifier et de se tester mutuellement.

Vous pouvez utiliser les messages Ping pour effectuer les tests suivants :

- Test de boucle avec retour de deux interfaces : vous pouvez initier l'envoi d'un message Ping d'une interface à une autre sur le même ASA, en tant que test de boucle avec retour externe pour vérifier l'état « opérationnel » de base et le fonctionnement de chaque interface.
- Envoyer un message Ping à un ASA : vous pouvez envoyer un message Ping à une interface sur un autre ASA pour vérifier qu'il est opérationnel et qu'il répond.

- Envoyer un message Ping via un ASA : vous pouvez envoyer un message Ping via un ASA intermédiaire en effectuant un Ping vers un périphérique situé de l'autre côté de l'ASA. Les paquets traverseront deux interfaces ASA intermédiaires dans chaque direction. Cette action effectue un test de base des interfaces, du fonctionnement et du temps de réponse de l'unité intermédiaire.
- Envoyer un message Ping pour tester le fonctionnement suspect d'un appareil réseau : vous pouvez envoyer un message Ping d'une interface ASA vers un appareil réseau que vous soupçonnez de fonctionner de manière incorrecte. Si l'interface est configurée correctement et qu'aucun écho n'est reçu, il pourrait y avoir des problèmes avec l'appareil.
- Envoyer un message Ping pour tester les communications intermédiaires : vous pouvez envoyer un message Ping à partir d'une interface ASA vers un appareil réseau connu pour fonctionner correctement. Si l'écho est reçu, le bon fonctionnement de tous les appareils intermédiaires et la connectivité physique sont confirmés.

Choisir entre le ping ICMP et TCP

L'ASA comprend le Ping traditionnel, qui envoie des paquets de requête d'écho ICMP et reçoit les paquets de réponse d'écho en retour. Il s'agit d'un outil standard qui fonctionne bien si tous les périphériques du réseau autorisent le trafic ICMP. Avec le Ping ICMP, vous pouvez envoyer un message Ping aux adresses IPv4 ou IPv6, ou aux noms d'hôte.

Cependant, certains réseaux interdisent le protocole ICMP. Si cela est le cas pour votre réseau, vous pouvez plutôt utiliser le Ping TCP pour tester la connectivité du réseau. Avec le Ping TCP, le Ping envoie des paquets TCP SYN et considère le Ping comme réussi s'il reçoit un SYN-ACK en réponse. Avec le Ping TCP, vous pouvez envoyer un message Ping à des adresses IPv4 ou à des noms d'hôte, mais vous ne pouvez pas envoyer un message Ping à des adresses IPv6.

Gardez à l'esprit qu'un message Ping ICMP ou TCP réussi signifie simplement que l'adresse que vous utilisez est active et répond à ce type de trafic. Cela signifie que la connectivité de base fonctionne. D'autres politiques exécutées sur un périphérique peuvent empêcher des types de trafic de passer avec succès par un périphérique.

Activer le protocole ICMP

Par défaut, vous pouvez envoyer un message Ping d'une interface à haute sécurité vers une interface à faible sécurité. Il vous suffit d'activer l'inspection ICMP pour permettre le trafic de retour. Si vous souhaitez effectuer un message Ping depuis une interface moins sécurisée vers une interface hautement sécurisée, vous devez appliquer une ACL pour autoriser le trafic.

Lors de l'envoi d'un message Ping à une interface ASA, toutes les règles ICMP appliquées à l'interface doivent autoriser les paquets de requête d'écho et de réponse d'écho. Les règles ICMP sont facultatives : si vous ne les configurez pas, tout le trafic ICMP vers une interface est autorisé.

Cette procédure explique toute la configuration ICMP que vous pourriez devoir effectuer pour activer l'envoi d'un message Ping ICMP des interfaces ASA ou pour l'envoi d'un message Ping par l'intermédiaire d'un ASA.

Procédure

Étape 1 Assurez-vous que les règles ICMP autorisent la requête d'écho/la réponse d'écho.

Les règles ICMP sont facultatives et s'appliquent aux paquets ICMP envoyés directement à une interface. Si vous n'appliquez pas de règles ICMP, tous les accès ICMP sont autorisés. Dans ce cas, aucune action n'est requise.

Cependant, si vous mettez en œuvre des règles ICMP, assurez-vous d'inclure des règles qui autorisent n'importe quelle adresse pour les messages d'écho et la réponse d'écho sur chaque interface. Configurez les règles ICMP dans le volet **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > ICMP**.

Étape 2 Assurez-vous que les critères d'accès autorisent le protocole ICMP.

Lors de l'envoi d'un message Ping à un hôte via un ASA, les critères d'accès doivent autoriser le trafic ICMP à sortir et à revenir. Le critère d'accès doit autoriser au moins les paquets ICMP de requête d'écho/réponse d'écho. Vous pouvez ajouter ces règles en tant que règles globales.

Si vous n'avez pas de critères d'accès, vous devrez également autoriser l'autre type de trafic souhaité, car l'application de critères d'accès à une interface ajoute un refus implicite, de sorte que tout autre trafic sera abandonné.

Configurez les critères d'accès dans le volet **Configuration > Firewall (Pare-feu) > Access Rules (Critères d'accès)**. Si vous ajoutez simplement les règles à des fins de test, vous pouvez les supprimer après avoir terminé les tests.

Étape 3 Activez l'inspection ICMP.

L'inspection ICMP est nécessaire lors de l'envoi d'un message Ping à l'ASA, par opposition à l'envoi d'un message Ping à une interface. L'inspection permet de renvoyer le trafic (c'est-à-dire le paquet de réponse d'écho) à l'hôte qui a initié le message Ping et garantit également qu'il y a une réponse par paquet, ce qui empêche certains types d'attaques.

Vous pouvez simplement activer l'inspection ICMP dans la politique d'inspection globale par défaut.

a) Choisissez **Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service)**.
b) Modifiez la règle globale **inspection_default**.
c) Dans l'onglet **Rule Actions (Actions de règles) > Protocol Inspection (Inspection de protocole)**, sélectionnez ICMP.
d) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Envoyer un message ping à des hôtes

Pour envoyer un message Ping à n'importe quel appareil, choisissez simplement **Tools (Outils) > Ping**, saisissez l'adresse IP ou le nom d'hôte de la destination à laquelle vous envoyez un message Ping, puis cliquez sur **Ping**. Pour le ping TCP, sélectionnez **TCP** et incluez également le port de destination. C'est généralement tout ce que vous avez à faire pour effectuer un test.

Exemple de sortie pour un envoyer un message Ping réussi :

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Si l'envoi d'un message Ping échoue, la sortie indique ? pour chaque tentative en échec, et le taux de réussite est inférieur à 100 % (un échec complet correspond à 0 %) :

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

Cependant, vous pouvez également ajouter des paramètres pour contrôler certains aspects du message Ping. Voici vos options de base :

- Ping ICMP : vous pouvez sélectionner l'interface utilisée pour l'adresse IP source; cependant, l'interface de sortie est déterminée par une recherche de routage à l'aide de la table de routage des données. Vous pouvez envoyer un message Ping aux adresses IPv4 ou IPv6 ou aux noms d'hôte.
- Ping TCP : vous devez également sélectionner le port TCP pour la destination à laquelle vous envoyez un ping. Par exemple, **www.example.com 80** pour envoyer un message Ping au port HTTP. Vous pouvez envoyer un message Ping à des adresses IPv4 ou à des noms d'hôte, mais pas aux adresses IPv6.

  Vous avez également la possibilité de spécifier l'interface utilisée pour l'adresse IP source; cependant, l'interface de sortie est déterminée par une recherche de routage à l'aide de la table de routage des données.

  Enfin, vous pouvez spécifier la fréquence de répétition du message Ping (la valeur par défaut est de 5 fois) ou le délai d'expiration pour chaque tentative (la valeur par défaut est de 2 secondes).

Tester la connectivité ASA de manière systématique

Si vous souhaitez effectuer un test plus systématique de la connectivité ASA, vous pouvez utiliser la procédure générale suivante.

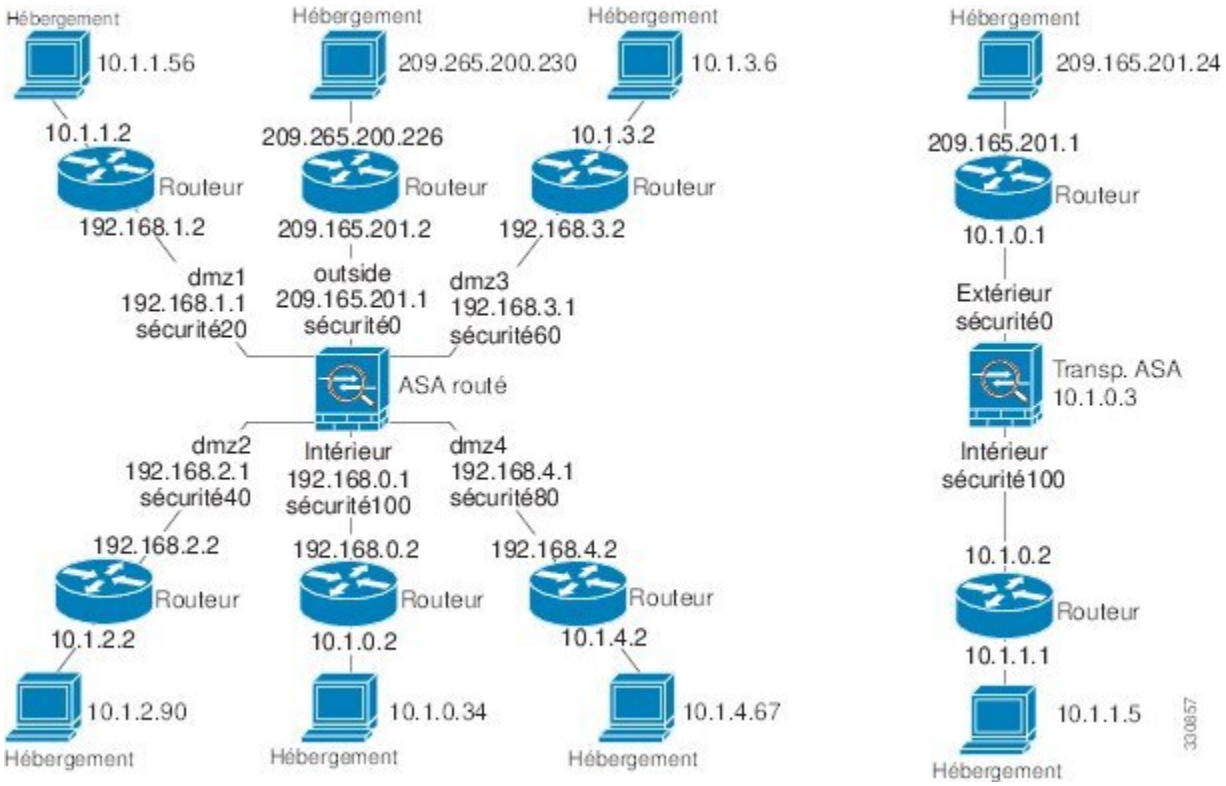
Avant de commencer

Si vous souhaitez voir les messages de journal système mentionnés dans la procédure, activez la journalisation (la commande **logging enable**, ou **Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Logging Setup (Configuration de la journalisation)** dans ASDM).

Procédure

Étape 1 Tracez un diagramme de votre ASA ou de votre contexte de sécurité en mode unique qui affiche les noms d'interface, les niveaux de sécurité et les adresses IP. Le diagramme doit également inclure tous les routeurs directement connectés et un hôte de l'autre côté du routeur à partir duquel vous allez envoyer un message Ping à l'ASA.

Illustration 93 : Diagramme de réseau avec interfaces, routeurs et hôtes



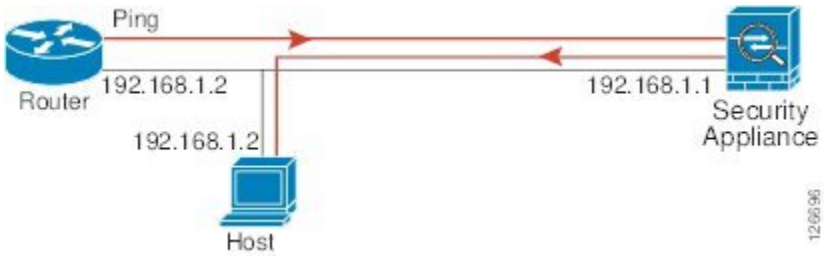
Étape 2 Envoyez un ping à chaque interface ASA à partir des routeurs directement connectés. Pour le mode transparent, envoyez un message Ping à l'adresse IP des BVI. Ce test garantit que les interfaces ASA sont actives et que la configuration d'interface est correcte.

Un message Ping peut échouer si l'interface ASA n'est pas active, si la configuration d'interface est incorrecte ou si un commutateur entre l'ASA et un routeur est en panne (voir la figure suivante). Dans ce cas, aucun message de débogage ni message de journal système ne s'affiche, car le paquet n'atteint jamais l'ASA.

Illustration 94 : Échec de ping à l'interface ASA



Illustration 95 : Échec de ping en raison de problèmes d'adressage IP



Si la réponse Ping ne revient pas au routeur, une boucle de commutation ou des adresses IP redondantes peuvent exister (voir la figure suivante).

Étape 3 Envoyez un ping à chaque interface ASA à partir d'un hôte distant. Pour le mode transparent, envoyez un message Ping à l'adresse IP des BVI. Ce test vérifie si le routeur connecté directement peut acheminer le paquet entre l'hôte et l'ASA et si l'ASA peut correctement acheminer le paquet vers l'hôte.

Un message Ping peut échouer si l'ASA n'a pas de route de retour vers l'hôte par le routeur intermédiaire (voir la figure suivante). Dans ce cas, les messages de débogage indiquent que l'envoi du message Ping a réussi, mais le message de journal système 110001 s'affiche, indiquant qu'une défaillance de routage s'est produite.

Illustration 96 : Échec de ping, car l'ASA n'a pas de route de retour



Étape 4 Envoyez un ping d'une interface ASA vers un périphérique réseau qui fonctionne correctement.

- Si le ping n'est pas reçu, il peut y avoir un problème avec le matériel de transmission ou la configuration de l'interface.
- Si l'interface ASA est configurée correctement et ne reçoit pas de réponse d'écho de l'appareil « connu pour être en bon état de fonctionnement », des problèmes avec la fonction de réception matérielle de l'interface peuvent exister. Si une interface différente ayant une capacité de réception « connue pour être bonne » peut recevoir un écho après avoir envoyé un message ping au même appareil « connu pour être bon », le problème de réception matérielle de la première interface est confirmé.

Étape 5 Envoyez un ping de l'hôte ou du routeur par l'interface source vers un autre hôte ou routeur sur une autre interface. Répétez cette étape pour autant de paires d'interfaces que vous souhaitez vérifier. Si vous utilisez la NAT, ce test montre que la NAT fonctionne correctement.

Si l'envoi d'un message Ping réussit, un message de journal système s'affiche pour confirmer la traduction d'adresses pour le mode routé (305009 ou 305011) et qu'une connexion ICMP a été établie (302020). Vous pouvez également saisir la commande **show xlate** ou **show conns** pour afficher ces renseignements.

L'envoi d'un message Ping peut échouer parce que la NAT n'est pas configurée correctement. Dans ce cas, un message de journal système s'affiche, indiquant que la NAT a échoué (305005 ou 305006). Si l'envoi d'un message Ping provient d'un hôte externe vers un hôte interne et que vous n'avez pas de traduction statique, vous recevez le message 106010.

Illustration 97 : Échec de ping parce que l'ASA ne traduit pas les adresses



Tracer les routes vers les hôtes

Si vous rencontrez des difficultés pour envoyer du trafic vers une adresse IP, vous pouvez tracer la route vers l'hôte pour déterminer s'il y a un problème sur le chemin réseau.

Procédure

Étape 1 Rendre l'ASA visible sur les routes de trace, à la page 1247.

Étape 2 Déterminer les routes de paquets, à la page 1247.

Rendre l'ASA visible sur les routes de trace

Par défaut, l'ASA n'apparaît pas sur les routes de trace en tant que saut. Pour l'afficher, vous devez décrémenter la durée de vie des paquets qui passent par l'ASA et augmenter la limite de débit pour les messages ICMP inaccessibles.

Procédure

Étape 1 Décrémentez la TTL à l'aide d'une politique de service.

a) Choisissez **Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service)**.
b) Ajoutez ou modifiez une règle. Par exemple, si vous avez déjà une règle à laquelle vous pouvez ajouter l'option de décrémentation de la TTL, vous n'avez pas besoin d'en créer une nouvelle.
c) Parcourez l'assistant jusqu'à la page Rule Actions (Actions découlant d'une règle), appliquez la règle globalement ou à une interface et spécifiez la correspondance de trafic. Par exemple, vous pouvez créer une règle de correspondance globale.
d) Sur la page Rule Actions (Actions découlant d'une règle), cliquez sur l'onglet **Connection Settings** (Paramètres de connexion) et sélectionnez **Decrement time to live for a connection** (Décrémenter la durée de vie d'une connexion).
e) Cliquez sur **OK** ou **Finish** (Terminer), puis **Apply** (Appliquer).

Étape 2 Augmentez la limite de débit pour les messages ICMP inaccessibles.

a) Choisissez **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > ICMP**.
b) Augmentez la valeur **IPv4 ICMP Unreachable Message Limits > Rate Limit** (Limites de messages ICMP inaccessibles IPv4 > Limite de débit) au bas de la page. Par exemple, augmentez-la à 50.
c) Cliquez sur **Apply** (Appliquer).

Déterminer les routes de paquets

Utilisez la route de trace pour vous aider à déterminer la route que les paquets emprunteront pour atteindre leur destination. Une route de trace fonctionne en envoyant des paquets UDP ou des échos ICMPv6 à une destination sur un port non valide. Comme le port n'est pas valide, les routeurs situés sur le chemin vers la

destination répondent par un message de dépassement de temps ICMP ou ICMPv6 et signalent cette erreur à l'ASA.

La route de trace affiche le résultat de chaque sonde envoyée. Chaque ligne de sortie correspond à une valeur TTL par ordre croissant. Le tableau suivant explique les symboles de sortie.

Symbole de sortie	Description
*	Aucune réponse n'a été reçue pour la sonde dans le délai d'expiration.
U	Aucune route vers la destination.
nn msec	Pour chaque nœud, le temps d'aller-retour (en millisecondes) pour le nombre spécifié de sondes.
!N.	Réseau ICMP inaccessible. Pour ICMPv6, l'adresse est hors du champ d'application.
!H	Hôte ICMP inaccessible.
!P	ICMP inaccessible. Pour ICMPv6, port inaccessible.
!A	ICMP administrativement interdit.
?	Erreur ICMP inconnue.

Procédure

Étape 1 Choisissez **Tools (Outils)** > **Traceroute (Route de trace)**.

Étape 2 Saisissez le nom d'hôte ou l'adresse IP de destination vers lesquels vous tracez la route. Configurez un serveur DNS pour utiliser un nom d'hôte.

Étape 3 (Facultatif) Configurez les caractéristiques de la trace. Les valeurs par défaut conviennent dans la plupart des cas.

- **Timeout** (Délai d'expiration) : durée d'attente d'une réponse avant expiration du délai. La valeur par défaut est de 3 secondes.
- **Port** : le port UDP à utiliser. La valeur par défaut est 33434.
- **Probe** (Sonde) : nombre de sondes à envoyer à chaque niveau TTL. La valeur par défaut est de 3.
- **TTL** : valeurs de durée de vie minimum et maximum pour les sondes. La valeur minimum par défaut est de 1, mais vous pouvez la définir à une valeur plus élevée pour supprimer l'affichage des sauts connus. La valeur par défaut est 30. La route de trace se termine lorsque le paquet atteint sa destination ou lorsque la valeur maximum est atteinte.
- **Specify source interface or IP address** (Spécifier l'interface source ou l'adresse IP) : l'interface à utiliser comme source de la trace. Vous pouvez définir l'interface par son nom ou par son adresse IP. Pour IPv6, vous ne pouvez pas spécifier l'interface source; vous pouvez uniquement spécifier l'adresse IP source. Une adresse IPv6 n'est valide que si vous avez activé IPv6 sur une interface ASA.En mode transparent, vous devez utiliser l'adresse de gestion.

- **Reverse Resolve** (Résolution inverse) : si vous souhaitez que la sortie affiche les noms des sauts rencontrés si la résolution de nom DNS est configurée. Désélectionnez l'option pour afficher uniquement les adresses IP.
- **Use ICMP** (Utiliser ICMP) : si vous souhaitez envoyer des paquets de sonde ICMP au lieu de paquets de sonde UDP.

Étape 4 Cliquez sur **Trace Route** (Route de trace) pour démarrer la route de trace.

La zone **Traceroute Output** (Sortie de la route de trace) affiche des messages détaillés sur les résultats de la route de trace.

Utiliser l'outil Packet Tracer pour tester la configuration de la politique

Vous pouvez tester la configuration de votre politique en modélisant un paquet basé sur des adresses source et de destination, et des caractéristiques de protocole. La trace effectue des recherches de politiques pour tester les critères d'accès, la NAT, le routage, etc., pour voir si le paquet est autorisé ou refusé.

En testant les paquets de cette manière, vous pouvez voir les résultats de vos politiques et vérifier si les types de trafic que vous souhaitez autoriser ou refuser sont gérés comme vous le souhaitez. En plus de vérifier votre configuration, vous pouvez utiliser le traceur pour déboguer un comportement inattendu, tel que le refus de paquets alors qu'ils devraient être autorisés.

Procédure

Étape 1 Choisissez **Tools (Outils)** > **Packet Tracer (Outil de trace de paquets)**.

Étape 2 Choisissez l'**Interface** source pour la trace de paquet.

Étape 3 Spécifiez le **Packet Type** (Type de paquet) pour la trace de paquet. Les types de protocole disponibles sont ICMP, IP, TCP, UDP, SCTP.

Étape 4 (Facultatif) Si vous souhaitez suivre un paquet dont la valeur de balise de groupe de sécurité est intégrée dans l'en-tête CMD de couche 2 (Trustsec), cochez la case **SGT number** (Numéro SGT) et saisissez le numéro de balise de groupe de sécurité, de 0 à 65 533.

Étape 5 (Mode transparent) Si vous souhaitez que le traceur de paquets entre dans une interface parent, qui est ensuite redirigée vers une sous-interface, cochez **VLAN ID** (ID de VLAN) et entrez l'ID, de 1 à 4 096. L'ID de VLAN est disponible uniquement lorsque l'interface d'entrée n'est pas une sous-interface.

Étape 6 (Mode transparent) Spécifiez la **Destination MAC Address** (Adresse MAC de destination).

Étape 7 Spécifiez la source et la destination des paquets.

Vous pouvez spécifier des adresses IPv4 ou IPv6, des noms de domaine complets (FQDN), des noms de groupes de sécurité ou des balises si vous utilisez Cisco Trustsec. Pour l'adresse source, vous pouvez également spécifier un nom d'utilisateur au format Domaine\nom d'utilisateur.

Étape 8 Spécifiez les caractéristiques du protocole :

- ICMP : saisissez le type ICMP, le code ICMP (0 à 255) et éventuellement l'identifiant ICMP.
- TCP/UDP/SCTP : saisissez les numéros de port source et de destination.

- Adresse IP brute : saisissez le numéro de protocole, de 0 à 255.

Étape 9 Utilisez le traceur de paquets pour déboguer les paquets sur les unités de grappe. Dans la liste déroulante **Cluster Capture** (Capture de grappe), sélectionnez :

a) **decrypted** : injecte un paquet déchiffré dans un tunnel VPN et simule également un paquet qui traverse un tunnel VPN.
b) **persist** : injecte le paquet dont vous souhaitez suivre les unités de grappe.
c) **bypass-checks** : ignore les vérifications de sécurité comme les ACL, les filtres VPN, l'usurpation d'adresse IPsec et uRPF.
d) **transmit** : autorise des paquets simulés à quitter l'ASA.

Étape 10 Cliquer sur **Start** (Démarrer) pour suivre le paquet.

Information Display Area (Zone d'affichage des renseignements) affiche des messages détaillés sur les résultats de la trace de paquet.

Supervision des performances et des ressources du système

Vous pouvez surveiller diverses ressources système pour déterminer les performances ou d'autres problèmes potentiels.

Supervision des performances

Vous pouvez afficher les informations sur les performances de l'ASA dans un format graphique ou tableau.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Connection Graphs (Graphiques de connexion)** > **Perfmon**.

Étape 2 Vous pouvez attribuer un titre à la fenêtre de graphique en le saisissant dans **Graph Window Title** (Titre de fenêtre de graphique), ou vous pouvez choisir un titre existant.

Étape 3 Sélectionnez jusqu'à quatre entrées dans la liste des graphiques disponibles, puis cliquez sur **Add** (Ajouter) pour les déplacer vers la liste des graphiques sélectionnés. Les options disponibles sont les suivantes :

- AAA Perfmon : demandes par seconde pour les demandes authentification, d'autorisation et de gestion de comptes.
- Inspection Perfmon : paquets par seconde pour l'inspection HTTP, FTP et TCP.
- Web Perfmon : demandes par seconde pour les demandes d'accès URL et de serveur d'URL.
- Connexions Perfmon : connexions par seconde pour toutes les connexions, les connexions UDP, les connexions TCP et l'interception TCP.
- Xlate Perfmon : xlates NAT par seconde.

Étape 4 Cliquez sur **Show Graphs** (Afficher les graphiques).

Vous pouvez faire basculer chaque graphique entre les affichages de graphique et de tableau. Vous pouvez également modifier la fréquence d'actualisation des données et exporter ou imprimer les données.

Supervision des blocs de mémoire

Vous pouvez afficher les renseignements sur les blocs de mémoire disponibles et utilisés dans un format graphique ou tableau.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **System Resources Graphs (Graphiques des ressources du système)** > **Blocks (Blocs)**.

Étape 2 Vous pouvez attribuer un titre à la fenêtre de graphique en le saisissant dans **Graph Window Title** (Titre de fenêtre de graphique), ou vous pouvez choisir un titre existant.

Étape 3 Sélectionnez des entrées dans la liste des graphiques disponibles, puis cliquez sur **Add** (Ajouter) pour les déplacer dans la liste des graphiques sélectionnés. Les options disponibles sont les suivantes :

- Blocs utilisés : affiche les blocs de mémoire utilisés de l'ASA.
- Blocs libres : affiche les blocs de mémoire libres de l'ASA.

Étape 4 Cliquez sur **Show Graphs** (Afficher les graphiques).

Vous pouvez faire basculer chaque graphique entre les affichages de graphique et de tableau. Vous pouvez également modifier la fréquence d'actualisation des données et exporter ou imprimer les données.

Supervision du CPU

Vous pouvez afficher l'utilisation du processeur.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **System Resources Graphs (Graphiques des ressources du système)** > **CPU**.

Étape 2 Vous pouvez attribuer un titre à la fenêtre de graphique en le saisissant dans **Graph Window Title** (Titre de fenêtre de graphique), ou vous pouvez choisir un titre existant.

Étape 3 Ajoutez l'utilisation du CPU à la liste des graphiques sélectionnés.

Étape 4 Cliquez sur **Show Graphs** (Afficher les graphiques).

Vous pouvez faire basculer le graphique entre les affichages de graphique et de tableau. Vous pouvez également modifier la fréquence d'actualisation des données et exporter ou imprimer les données.

Supervision de la mémoire

Vous pouvez afficher les renseignements d'utilisation de la mémoire dans un format graphique ou tableau.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **System Resources Graphs (Graphiques des ressources du système)** > **Memory (Mémoire)**.

Étape 2 Vous pouvez attribuer un titre à la fenêtre de graphique en le saisissant dans **Graph Window Title** (Titre de fenêtre de graphique), ou vous pouvez choisir un titre existant.

Étape 3 Sélectionnez des entrées dans la liste des graphiques disponibles, puis cliquez sur **Add** (Ajouter) pour les déplacer dans la liste des graphiques sélectionnés. Les options disponibles sont les suivantes :

- Mémoire libre : affiche la mémoire libre de l'ASA.
- Mémoire utilisée : affiche la mémoire utilisée de l'ASA.

Étape 4 Cliquez sur **Show Graphs** (Afficher les graphiques).

Vous pouvez faire basculer chaque graphique entre les affichages de graphique et de tableau. Vous pouvez également modifier la fréquence d'actualisation des données et exporter ou imprimer les données.

Supervision de l'utilisation du CPU par processus

Vous pouvez superviser les processus qui s'exécutent sur le CPU. Vous pouvez obtenir des renseignements sur le pourcentage de CPU utilisé par un processus donné. Les statistiques d'utilisation du CPU sont triées par ordre décroissant pour afficher le consommateur le plus élevé en haut. Des renseignements concernant la charge sur le CPU par processus sont également inclus, 5 secondes, 1 minute et 5 minutes avant l'heure du journal. Ces renseignements sont mis à jour automatiquement toutes les 5 secondes pour fournir des statistiques en temps réel. Dans ASDM, ils sont mis à jour toutes les 30 secondes.

Pour afficher l'utilisation du CPU par processus, choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Per-Process CPU Usage (Utilisation du CPU par processus)**.

Vous pouvez arrêter l'actualisation automatique, actualiser manuellement les renseignements ou les enregistrer dans un fichier. Vous pouvez également cliquer sur **Configure CPU Usage Colors** (Configurer les couleurs d'utilisation du CPU) pour choisir des couleurs d'arrière-plan et de premier plan en fonction des pourcentages d'utilisation, afin de faciliter l'analyse des processus à utilisation élevée.

Supervision des connexions

Pour afficher les connexions actuelles sous forme de tableau, dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision) > Properties (Propriétés) > Connections (Connexions)**. Les renseignements relatifs à chaque connexion comprennent les caractéristiques du protocole, des adresses source et de destination, le temps d'inactivité depuis l'envoi ou la réception du dernier paquet, ainsi que le volume de trafic dans la connexion.

Historique des tests et du dépannage

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge IPv6 pour les routes de trace	9.7(1)	La commande **traceroute** a été modifiée pour accepter une adresse IPv6. Nous avons modifié l'écran suivant : **Tools (Outils)** > **Traceroute (Route de trace)**
Prise en charge de l'outil de trace de paquets pour les interfaces membres du groupe de ponts	9.7(1)	Vous pouvez désormais utiliser l'outil de trace de paquets pour les interfaces membres d'un groupe de ponts. Nous avons ajouté les champs **VLAN ID** (ID de VLAN) et **Destination MAC Address** (Adresse MAC de destination) dans l'écran de l'outil de trace de paquets :**Tools (Outils)** > **Packet Tracer (Outil de trace de paquets)**
Démarrer et arrêter manuellement les captures de paquets	9.7(1)	Vous pouvez maintenant arrêter et démarrer manuellement la capture. Écrans ajoutés ou modifiés : **Wizards (Assistants)** > **Packet Capture Wizard (Assistant de capture de paquets)** > **Run Captures (Exécuter des captures)** Options ajoutées ou modifiées : bouton **Start** (Démarrer), bouton **Stop** (Arrêter)

Nom de la caractéristique	Versions de plateforme	Description
Capacités améliorées de l'outil de trace de paquets et de la capture de paquets	9.9(1)	L'outil de trace de paquets a été amélioré avec les fonctionnalités suivantes : • Tracer un paquet lorsqu'il passe entre les unités de grappe. • Autoriser des paquets simulés à quitter l'ASA. • Contourner les contrôles de sécurité pour un paquet simulé. • Considérer un paquet simulé comme un paquet IPsec/SSL déchiffré. La capture de paquets a été améliorée avec les fonctionnalités suivantes : • Capturer les paquets après leur déchiffrement. • Capturer les traces et les conserver dans la liste persistante. Écrans nouveaux ou modifiés : **Tools (Outils)** > **Packet Tracer (Outil de trace de paquets)** Nous avons ajouté le champ **Cluster Capture** (Capture de grappe) pour prendre en charge les options suivantes : **decrypted**, **persist**, **bypass-checks**, **transmit** Nous avons ajouté deux nouvelles options dans la vue **Filter By** (Filtrer par) dans la liste déroulante **All Sessions** (Toutes les sessions) : **Origin** et **Origin-ID** **Monitoring (Supervision)** > **VPN** > **VPN Statistics (Statistiques de VPN)** > **Packet Tracer and Capture (Outil de trace et capture de paquets)** Nous avons ajouté le champ **ICMP Capture** (Capture ICMP) dans l'écran Packet Capture Wizard (Assistant de capture de paquets) :**Wizards (Assistants)** > **Packet Capture Wizard (Assistant de capture de paquets)** Nous avons ajouté deux options : **include-decrypted** et **persist** pour prendre en charge la capture ICMP.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de la capture de paquets pour le trafic IPv6 correspondant sans l'utilisation d'une ACL	9.10(1)	Si vous utilisez le mot clé **match** pour la commande **capture**, le mot clé **any** ne correspond qu'au trafic IPv4. Vous pouvez désormais spécifier les mots clés **any4** et **any6** pour capturer le trafic IPv4 ou IPv6. Le mot clé **any** continue de correspondre uniquement au trafic IPv4. Commandes nouvelles ou modifiées : **capture match** ASDM n'est pas pris en charge.
Nouvelle commande **debug telemetry** pour Forepower 9300/4100.	9.14(1)	Si vous utilisez la commande **debug telemetry**, les messages de débogage liés à la télémétrie s'affichent. Les débogages aident à identifier la cause des erreurs lors de la génération du rapport de télémétrie. Aucun écran modifié.
Modifications de la commande **ping**	9.18(2)	Pour prendre en charge l'envoi d'un message ping à une interface de boucle avec retour, la commande **ping** a maintenant changé de comportement. Si vous spécifiez l'interface dans la commande, l'adresse IP source correspond à l'adresse IP de l'interface spécifiée, mais l'interface de sortie réelle est déterminée par une recherche de route à l'aide de la table de routage des données. Commandes nouvelles ou modifiées : **ping**



PARTIE VIII

Surveillance

- Journalisation, à la page 1259
- MIB SNMP, à la page 1299
- Données de télémétrie et du Cisco Success Network, à la page 1321
- Alarmes pour Cisco ISA 3000, à la page 1331
- Rapports anonymes et Smart Call Home, à la page 1337



CHAPITRE 48

Journalisation

Ce chapitre décrit comment consigner les messages système et les utiliser pour la résolution de problèmes.

- À propos de la journalisation, à la page 1259
- Lignes directrices relatives à la journalisation, à la page 1267
- Configurer la journalisation, à la page 1269
- Supervision des journaux, à la page 1291
- Historique de journalisation, à la page 1296

À propos de la journalisation

La journalisation du système est une méthode de collecte de messages des périphériques vers un serveur exécutant un daemon syslog. La journalisation sur un serveur syslog central facilite l'agrégation des journaux et des alertes. Les périphériques Cisco peuvent envoyer leurs messages de journal à un service syslog de type UNIX. Un service syslog accepte les messages et les stocke dans des fichiers ou les imprimés conformément à un fichier de configuration simple. Cette forme de journalisation offre un stockage protégé à long terme pour les journaux. Les journaux sont utiles pour les dépannages de routine et pour le traitement des incidents.

Les journaux système d'ASA vous fournissent des renseignements pour superviser et dépanner l'ASA. La fonction de journalisation vous permet d'effectuer les opérations suivantes :

- Spécifier quels messages du journal système doivent être enregistrés.
- Désactiver ou modifier le niveau de gravité d'un message du journal système.
- Préciser au moins un emplacement où les messages du journal système doivent être envoyés, notamment :
  - Un tampon interne
  - Un ou plusieurs serveurs de journal système
  - ASDM
  - Une station de gestion SNMP
  - Des adresses courriel spécifiées
  - Console
  - Sessions Telnet et SSH.

- Configurer et gérer les messages de journal système en groupes, par exemple par niveau de gravité ou classe de message.
- Spécifier si une limite de débit est appliquée ou non à la génération du journal système.
- Préciser ce qu'il arrive au contenu du tampon du journal interne lorsqu'il est plein : écraser le tampon, envoyer le contenu du tampon à un serveur FTP ou enregistrer le contenu dans la mémoire flash interne.
- Filtrer les messages du journal système par emplacements, niveau de gravité, classe ou liste de messages sur mesure.

Journalisation dans le mode de contexte multiple

Chaque contexte de sécurité comprend sa propre configuration de journalisation et génère ses propres messages. Si vous vous connectez au contexte de système ou d'administration, puis passez à un autre contexte, les messages que vous affichez dans votre session ne sont que les messages liés au contexte actuel.

Les messages de journal système qui sont générés dans l'espace d'exécution du système, y compris les messages de basculement, sont consultés dans le contexte d'administration avec les messages générés dans le contexte d'administration. Vous ne pouvez pas configurer la journalisation ni afficher des renseignements de journalisation dans l'espace d'exécution du système.

Vous pouvez configurer l'ASA pour inclure le nom de contexte dans chaque message, ce qui vous aide à différencier les messages de contexte qui sont envoyés à un seul serveur de journal système. Cette fonctionnalité vous aide également à déterminer quels messages proviennent du contexte d'administration et lesquels proviennent du système. Les messages qui proviennent de l'espace d'exécution du système utilisent un ID de périphérique de **système**, et les messages qui proviennent du contexte d'administration utilisent le nom du contexte d'administration comme ID de périphérique.

Analyse des messages du journal système

Voici quelques exemples du type de renseignements que vous pouvez obtenir en examinant différents messages du journal système :

- Les connexions autorisées par les politiques de sécurité d'ASA. Ces messages vous aident à repérer les failles qui restent ouvertes dans vos politiques de sécurité.
- Les connexions refusées par les politiques de sécurité d'ASA. Ces messages indiquent quels types d'activités sont dirigées vers votre réseau interne sécurisé.
- L'utilisation de la fonctionnalité de journalisation du taux de refus ACE affiche les attaques qui se produisent sur votre ASA.
- Les messages d'activité d'IDS peuvent afficher les attaques qui se sont produites.
- L'authentification de l'utilisateur et l'utilisation des commandes fournissent une piste d'audit des modifications des politiques de sécurité.
- Les messages d'utilisation de la bande passante affichent chaque connexion qui a été établie et détruite, ainsi que la durée et le volume de trafic utilisés.
- Les messages d'utilisation des protocoles affichent les protocoles et les numéros de port utilisés pour chaque connexion.

- Les messages de piste d'audit de traduction d'adresses enregistrent les connexions NAT ou PAT en cours d'établissement ou de destruction, ce qui est utile si vous recevez un rapport des activités malveillantes provenant de l'intérieur de votre réseau vers l'extérieur.

Format des messages du journal système

Les messages du journal système sont structurés comme suit :

```
[<PRI>]: [Timestamp] [Device-ID] : %-Level-Message_number: Message_text
```

Les descriptions des champs sont les suivantes :

<PRI>	Valeur de la priorité. Lorsque la journalisation EMBLEM est activée, cette valeur s'affiche dans le message de journal système. La journalisation EMBLEM est compatible avec UDP et non avec TCP.
Horodatage	La date et l'heure de l'événement s'affichent. Lorsque la journalisation des horodatages est activée, et si l'horodatage est configuré pour être au format RFC 5424, tous les horodatages dans les messages de journal système affichent l'heure en heure UTC, comme indiqué par la norme RFC 5424.
Device-ID	La chaîne d'identifiant du périphérique qui a été configurée lors de l'activation de l'option logging device-id par l' interface utilisateur. Si cette option est activée, l'ID de périphérique n'apparaît pas dans les messages de journal système au format EMBLEM.
	Le code d'installation du message de journal système pour les messages générés par l'. .
Level (Niveau)	Le niveau reflète la gravité de la condition décrite par le message de journal système : plus le nombre est bas, plus la condition est critique.
Message_number	Un numéro à six chiffres unique qui identifie le message de journal système.
Message_text	Une chaîne de texte qui décrit la condition. Cette partie du message de journal système comprend parfois des adresses IP, des numéros de port ou des noms d'utilisateurs.

Tous les messages de journal système générés par le périphérique sont documentés dans le guide Messages de journal système de la série Cisco Secure Firewall ASA.

Le format syslog EMBLEM est une convention propre à Cisco, fondée sur les normes RFC 3164 et RFC 5424. Ainsi, lorsque EMBLEM est activé, le message syslog affiche deux-points (:) après le champ <PRI>.

Exemple de message de journal système avec la journalisation EMBLEM, la journalisation de l'horodatage RFC 5424 et l'ID de périphérique activés. Notez les deux-points (:) après le champ <PRI> (*<166>*).

```
<166>:2018-06-27T12:17:46Z: %-6-110002 : échec de localisation de l'interface de sortie
pour le protocole de l'interface src : port IP/src à l'adresse IP/au port de destination
```

Exemple de message de journal système avec la journalisation de l'horodatage RFC 5424 et l'ID de périphérique activés. Il n'y a pas de deux-points (:) avant l'horodatage.

```
2018-06-27T12:17:46Z  : %-6-110002 : échec de localisation de l'interface de sortie pour
le protocole de l'interface src : port IP/src à l'adresse IP/au port de destination
```

Niveaux de gravité des messages Syslog

Les niveaux de gravité des messages syslog définissent l'importance des messages système. Vous pouvez affecter des couleurs personnalisées à chacun des niveaux de gravité pour faciliter leur distinction dans les visualiseurs de journaux ASDM. Pour configurer les paramètres de couleur des messages du journal système, sélectionnez l'onglet **Outils > Préférences » Syslog** ou, dans la visionneuse de journal elle-même, cliquez sur **Paramètres de couleur** dans la barre d'outils.

Tableau 60 : Niveaux de gravité des messages Syslog

Numéro de niveau	Niveau de gravité	Description
0	**urgences**	Vous ne pouvez pas utiliser le système.
1	**alerte**	Vous devez agir immédiatement.
2	**critique**	Le système présente des conditions critiques à traiter.
3	**erreur**	Conditions d'erreur.
4	**avertissement**	Le système comporte des avertissements que vous devez consulter.
5	**notification**	Le système signale les événements importants que vous devez superviser.
6	**renseignements**	Messages informatifs seulement.
7	**débogage**	Le système génère uniquement des messages de débogage. Ne journalisez à ce niveau que temporairement, lors du débogage des problèmes. Ce niveau de journalisation peut générer de nombreux messages, ce qui peut affecter les performances du système.

Remarque ASA ne génère pas de messages syslog avec un niveau de gravité établi à zéro (urgences).

Filtres de messages syslog

Critères de filtrage des messages Syslog

Vous pouvez diriger les messages syslog vers une destination de sortie en fonction des critères suivants :

- Numéros d'ID des messages Syslog
- Niveau de gravité des messages du journal système
- Classe de messages Syslog (équivalente à une zone fonctionnelle)

Vous pouvez créer une liste de messages avec des critères spécifiques, que vous pouvez ensuite préciser lorsque la destination de la sortie est définie. Sinon, vous pouvez configurer les ASA pour envoyer une classe de messages particulière à chaque type de destination de sortie indépendamment de la liste de messages.

Classes de messages syslog et numéros d'ID de messages associés

Vous pouvez utiliser les classes de messages syslog de deux manières :

- Précisez un emplacement de sortie pour toute une catégorie de messages du journal système.
- Créez une liste de messages qui spécifie la classe du message.

Utilisez la classe de messages syslog pour catégoriser les messages syslog par type, comme les fonctionnalités ou les fonctions du périphérique. Par exemple, utilisez la classe RIP pour le routage RIP.

Tous les messages syslog d'une classe particulière partagent les trois mêmes chiffres initiaux dans leurs numéros d'ID de message syslog. Par exemple, les messages syslog pour la fonctionnalité de client VPN utilisent les numéros d'ID de 611101 à 611323.

La plupart des messages syslog ISAKMP comprennent des objets ajoutés au début qui identifient le tunnel. Ces objets précèdent le texte descriptif d'un message syslog lorsqu'ils sont disponibles. Si l'objet est inconnu lorsque le message syslog est généré, la combinaison d'en-tête et de valeur est omise.

Les objets sont préfixés de cette manière :

Group = *groupname*, Username = *user*, IP = *IP_address*

Le terme « groupe » ici fait référence à la configuration de groupe de tunnel. Le nom d'utilisateur provient de la base de données locale ou du serveur AAA. Il s'agit de l'adresse IP publique du client d'accès à distance ou de l'homologue de couche 2.

Le tableau suivant répertorie les classes de messages et la plage d'ID de message dans chaque classe.

Tableau 61 : Classes de messages syslog et numéros d'ID de messages associés

Classe	Définition	Numéros d'ID des messages Syslog
auth	Authentification de l'utilisateur	109, 113
—	Listes d'accès	106
—	Pare-feu d'application	415
—	Filtre de trafic de réseau de zombies	338
bridge (pont)	Pare-feu transparent	110, 220
ca	Autorité de certification de l'infrastructure de clé publique (PKI)	717
citrix	Client Citrix	723
—	Mise en grappe	747
—	Gestion des cartes	323

Classe	Définition	Numéros d'ID des messages Syslog
config (configurer)	Interface de commande	111, 112, 208, 308
csd	Poste de travail sécurisé	724
cts	TrustSec de Cisco	776
DAP	Politiques d'accès dynamique	734
EAP, eapoudp	EAP ou EAPoUDP pour le contrôle d'admission au réseau	333, 334
EIGRP	Routage EIGRP	336
e-mail	Serveur mandataire de courriel	719
—	Surveillance de l'environnement	735
ha	Basculement	101, 102, 103, 104, 105, 210, 311, 709
—	Pare-feu basé sur l'identité	746
ids	Système de détection des intrusions	400, 733
—	Boîte à outils IKEv2	750, 751, 752
IP	Pile d'adresse IP	209, 215, 313, 317, 408
ipaa	Affectation d'adresse IP	735
ips	Système de protection contre les intrusions	400, 401, 420
—	IPv6	325
—	Licence	444
MDM-proxy	Mandataire MDM	802
NAC	Contrôle d'admission au réseau (NAC)	731, 732
nacpolicy	Politique NAC	731
nacsettings	Paramètres NAC pour appliquer la politique NAC	732
—	NAT et PAT	305
—	Point d'accès réseau	713
NP	Processeur de réseau	319
—	NP SSL	725

Classe	Définition	Numéros d'ID des messages Syslog
OSPF	Routage OSPF	318, 409, 503, 613
—	Chiffrement de mot de passe	742
—	Serveur mandataire téléphonique	337
RIP	Routage RIP	107, 312
rm	Gestionnaire des ressources	321
—	Smart Call Home	120
séance de formation	Séance d'utilisateur	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
SNMP	SNMP	212
—	ScanSafe	775
SSL	Pile SSL	725
svc	Client VPN SSL	722
sys	Système	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
—	Détection des menaces	733
tag-switching	Commutation de balise de service	779
transactional-rule-engine-tre	Moteur de règles transactionnelles	780
uc-IMS	UC-IMS	339
vm	Mise en correspondance VLAN	730
vpdn	Sessions PPTP et L2TP	213, 403, 603
VPN	IKE et IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	Client VPN	611
vpnfo	Basculement du VPN	720
vpnlb	Équilibrage de la charge VPN	718
—	VXLAN	778
webfo	Basculement WebVPN	721

Classe	Définition	Numéros d'ID des messages Syslog
webvpn	WebVPN et Secure Client (services client sécurisés)	716

Trier les messages dans les visionneuses de journaux

Vous pouvez trier les messages dans toutes les visionneuses de journaux ASDM (c'est-à-dire la visionneuse de journaux en temps réel, la visionneuse de tampons de journaux et la dernière visionneuse d'événements du journal système ASDM). Pour trier les tableaux en fonction de plusieurs colonnes, cliquez sur l'en-tête de la première colonne que vous souhaitez trier, puis maintenez la touche **Ctrl** enfoncée et cliquez simultanément sur les en-têtes des autres colonnes que vous souhaitez inclure dans l'ordre de tri. Pour trier les messages par ordre chronologique, sélectionnez les colonnes de date et d'heure; sinon, les messages sont triés uniquement par date (peu importe l'heure) ou uniquement par heure (peu importe la date).

Lorsque vous triez des messages dans la visionneuse de journaux en temps réel et dans la dernière visionneuse d'événements du journal système ASDM, les nouveaux messages qui arrivent apparaissent dans l'ordre de tri, et non en haut, comme c'est normalement le cas. Autrement dit, ils sont mélangés avec les autres messages.

Listes de messages personnalisés

La création d'une liste de messages personnalisée est un moyen flexible d'exercer un contrôle sur les messages du journal système qui sont envoyés vers une destination de sortie spécifique. Dans une liste de messages de journal système personnalisée, vous spécifiez des groupes de messages de journal système à l'aide d'un ou de tous les critères suivants :

- Niveau de gravité
- ID du message
- Plages d'ID des messages du journal système
- Classe de messages.

Par exemple, vous pouvez utiliser des listes de messages pour effectuer les opérations suivantes :

- Sélectionnez les messages du journal système avec les niveaux de gravité 1 et 2 et envoyez-les à une ou plusieurs adresses courriel.
- Sélectionnez tous les messages du journal système associés à une classe de messages (comme ha) et enregistrez-les dans le tampon interne.

Une liste de messages peut inclure plusieurs critères de sélection des messages. Cependant, vous devez ajouter chaque critère de sélection des messages à l'aide d'une nouvelle entrée de commande. Il est possible de créer une liste de messages qui comprend des critères de sélection des messages qui se chevauchent. Si deux critères d'une liste de messages sélectionnent le même message, le message est journalisé une seule fois.

Mise en grappe

Les messages du journal système sont un outil inestimable pour la comptabilité, la surveillance et le dépannage dans un environnement de grappe. Chaque unité ASA de la grappe (jusqu'à huit unités sont autorisées) génère

des messages de journal système de manière indépendante; certaines commandes **logging** vous permettent ensuite de contrôler les champs d'en-tête, qui comprennent un horodatage et un ID de périphérique. Le serveur de journal système utilise l'ID de périphérique pour identifier le générateur de journaux systèmes. Vous pouvez utiliser la commande **logging device-id** pour générer des messages de journal système avec des ID de périphérique identiques ou différents afin de faire apparaître les messages comme provenant d'unités identiques ou différentes dans la grappe.



Remarque Pour superviser les messages de journal système provenant des unités d'une grappe, vous devez ouvrir une session ASDM pour chacune des unités que vous souhaitez superviser.

Lignes directrices relatives à la journalisation

Restrictions pour la journalisation IPv6

- IPv6 est pris en charge. Un message syslog peut être envoyé à l'aide de TCP ou d'UDP.
- Assurez-vous que l'interface configurée pour l'envoi des journaux système est activée, qu'elle est compatible avec IPv6, et que le serveur syslog est accessible par l'intermédiaire de l'interface désignée.
- Vous ne pouvez pas utiliser IPv6 pour une journalisation sécurisée.

Lignes directrices relatives à la configuration du serveur syslog

- Le serveur syslog doit exécuter un programme de serveur appelé syslogd. Windows fournit un serveur syslog dans le cadre de son système d'exploitation.
- Le serveur syslog fonctionne selon le processus syslog-ng du système de pare-feu. N'utilisez pas de fichiers de configuration externes, comme le fichier *scwx.conf* de SecureWorks. Étant donné que ces fichiers ne sont pas compatibles avec le périphérique, leur utilisation entraîne des erreurs d'analyse et l'échec du processus syslog-ng.
- Vous pouvez configurer jusqu'à seize serveurs de journaux système. Cependant, en mode contexte multiple, la limitation est de 4 serveurs par contexte.
- Attribuez une seule liste ou classe à chaque serveur syslog et emplacement.
- Le serveur syslog doit être accessible au moyen de l'ASA. Vous devez configurer le périphérique pour refuser les messages ICMP unreachable (ICMP injoignable) sur l'interface par laquelle le serveur syslog est accessible et pour envoyer des journaux syslog au même serveur. Activez la journalisation pour tous les niveaux de gravité. Pour éviter que le serveur syslog ne se bloque, supprimez la génération des syslogs 313001, 313004 et 313005.
- Pour afficher les journaux générés par ASA, vous devez spécifier une destination de sortie de journalisation. Si vous activez la journalisation sans préciser de destination de sortie de journalisation, l'ASA génère des messages mais ne les enregistre pas à un emplacement à partir duquel vous pouvez les afficher. Vous devez spécifier chaque destination de sortie de journalisation séparément. Par exemple, pour désigner plusieurs serveurs syslog comme destination de sortie, et spécifiez des entrées distinctes dans le volet **Serveur Syslog** pour chaque serveur syslog.

- Pour une journalisation sécurisée, le Syslog Firewall Threat Defense prend en charge le protocole TLS unidirectionnel. Il ne prend pas en charge l'authentification par certificat client, la configuration de point de confiance pour syslog ou le protocole TLS mutuel (certificat X.509).
- Le certificat de serveur reçu d'un serveur Syslog doit contenir « ServAuth » dans le champ Extended Key Usage (Utilisation de la clé étendue). Cette vérification sera effectuée uniquement pour les certificats non autosignés. Les certificats autosignés ne fournissent aucune valeur dans ce champ.

Interfaces pour la configuration du journal système

- Détermination de l'interface de sortie (egress) pour le syslog :
  - Si l'interface de gestion uniquement indiquée a l'accès de gestion activé, le centre de gestion effectuera des recherches dans le tableau de routage et déterminera l'interface de sortie (peut être des données ou une gestion) en fonction de la meilleure logique de routage.
  - Si vous configurez une interface de gestion uniquement en tant qu'hôte de journalisation, qui n'a pas d'accès de gestion activé, le centre de gestion utilisera l'interface, quelles que soient les entrées de la table de routage.

    Ainsi, pour que le centre de gestion utilise toujours un chemin de gestion dédié pour le trafic syslog, configurez l'interface de gestion sans accès de gestion, puis précisez l'interface dans l'hôte de journalisation :

    ```
    interface <management-interface>
    management-only ----->Do not include management-access
    logging host <management-interface> <syslog-server-ip>
    ```

- Lorsque le débit syslog dépasse 50 000 messages par seconde, veillez à utiliser une interface de données comme interface de sortie plutôt qu'une interface de gestion.
- Lorsque vous utilisez une liste de messages personnalisée pour correspondre uniquement aux résultats de liste d'accès, les journaux de liste d'accès ne sont pas générés pour les listes dont le niveau de gravité de journalisation a été augmenté à débogage (niveau 7). Le niveau de gravité de la journalisation par défaut est défini à 6 pour la commande **logging list** (liste de journalisation). Ce comportement par défaut a été prévu. Lorsque vous modifiez explicitement le niveau de gravité de la journalisation de la configuration de la liste d'accès à Débogage, vous devez également modifier la configuration de journalisation elle-même.

  Voici un exemple de sortie de la commande **show running-config logging** qui n'inclut pas les résultats de la liste d'accès, car leur niveau de gravité de journalisation a été remplacé par « débogage » :

  ```
  ciscoasa# show running-config logging
  logging enable
  logging timestamp
  logging list test message 106100
  logging buffered test
  ```

  Voici un exemple de sortie de la commande **show running-config logging** qui inclut les résultats de la liste d'accès :

  ```
  ciscoasa# show running-config logging
  logging enable
  logging timestamp
  logging buffered debugging
  ```

Dans ce cas, la configuration de la liste d'accès ne change pas et le nombre d'occurrences de la liste d'accès s'affiche, comme le montre l'exemple suivant :

```
ciscoasa(config)# access-list global line 1 extended
permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended
permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

Connexions TCP et UDP pour syslog

- L'envoi de journaux du système sur TCP n'est pas pris en charge sur un périphérique de secours.
- Si vous utilisez TCP comme protocole de transport, le système ouvre quatre connexions au serveur syslog pour s'assurer que les messages ne sont pas perdus. Si vous utilisez le serveur syslog pour collecter les messages d'un très grand nombre de périphériques et que le surdébit de la connexion combinée est trop important pour le serveur, utilisez plutôt UDP.
- Le nombre de connexions UDP pour syslog est directement lié au nombre de CPU sur la plateforme matérielle et au nombre de serveurs syslog que vous configurez. À tout moment, il peut y avoir autant de connexions syslog UDP qu'il y a de CPU multiplié par le nombre de serveurs syslog configurés. Notez que le délai d'inactivité de la connexion UDP globale s'applique à ces sessions et que la valeur par défaut est de 2 minutes. Vous pouvez ajuster ce paramètre si vous souhaitez fermer ces sessions plus rapidement, mais le délai d'expiration s'applique à toutes les connexions UDP, pas seulement au syslog. Il s'agi du comportement prévu.
- Lorsque ASA envoie des journaux système via TCP, la connexion prend environ une minute pour s'établir après le redémarrage du service syslogd.
- Lorsque l'hôte de journalisation TCP tombe en panne, il faut environ 6 minutes pour faire passer son état de connexion de *Connected* (Connecté) à *Not connected* (Non connecté). La journalisation s'appuie sur le TCP pour détecter l'état du canal; jusqu'à ce moment-là, la journalisation envoie les journaux par le canal. Pendant ce temps, lorsque vous exécutez **show log**, la sortie affiche l'hôte de journalisation TCP comme connecté. Une fois que le canal TCP est fermé, l'état de l'hôte de journalisation TCP est mis à jour à *Not connected* (Non connecté).

Configurer la journalisation

Cette section décrit comment configurer la journalisation.

Activer la journalisation

Pour activer la journalisation, procédez comme suit :

Procédure

Étape 1 Dans ASDM, choisissez l'une des options suivantes :

- **Home (Accueil)** > **Latest ASDM Syslog Messages (Derniers messages du journal système ASDM)** > **Enable Logging (Activer la journalisation)**
- **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)**
- **Monitoring (Supervision)** > **Real-Time Log Viewer (Visionneuse de journal en temps réel)** > **Enable Logging (Activer la journalisation)**
- **Monitoring (Supervision)** > **Log Buffer (Tampon de journal)** > **Enable Logging (Activer la journalisation)**

Étape 2 Cochez la case **Enable logging** (Activer la journalisation) pour activer la journalisation.

Configurer une destination de sortie

Pour optimiser l'utilisation des messages de journal système pour le dépannage et la surveillance des performances, nous vous conseillons de préciser un ou plusieurs emplacements où les messages de journal système doivent être envoyés, y compris un tampon de journal interne, un ou plusieurs serveurs de journal système externes, ASDM, une station de gestion SNMP, le port de console, des adresses courriel spécifiées ou des sessions Telnet et SSH.

Lorsque vous configurez la journalisation syslog sur une interface avec accès de gestion uniquement activé, les journaux liés au plan de données (ID du journal système 302015, 302014, 106023 et 304001) sont abandonnés et n'atteignent pas le serveur de journal système. Les messages du journal système sont abandonnés, car la table de routage du chemin d'accès ne dispose pas du routage de l'interface de gestion. Par conséquent, assurez-vous que l'accès réservé à la gestion est désactivé sur l'interface que vous configurez.

Envoyer des messages du journal système à un serveur externe de journal système

Vous pouvez archiver les messages en fonction de l'espace disque disponible sur le serveur de journal système externe et manipuler les données de journalisation après leur enregistrement. Par exemple, vous pouvez préciser les actions à exécuter lorsque certains types de messages Syslog sont enregistrés, extraire les données du journal et enregistrer les enregistrements dans un autre fichier pour créer des rapports ou suivre les statistiques à l'aide d'un script spécifique au site.

Pour envoyer des messages de journal système à un serveur de journal système externe, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)**.

Étape 2 Cochez la case **Enable logging** (Activer la journalisation) pour activer la journalisation pour l'ASA.

Étape 3 Cochez la case **Enable logging on the failover standby unit** (Activer la journalisation sur l'unité de secours de basculement) pour activer la journalisation de l'ASA de secours, si disponible.

Étape 4 Cochez la case **Send debug messages as syslogs** (Envoyer les messages de débogage sous forme de journaux système) pour rediriger toute la sortie de trace de débogage vers les journaux système. Le message du journal système ne s'affiche pas sur la console si cette option est activée. Par conséquent, pour afficher les messages

de débogage, vous devez activer la journalisation sur la console et la configurer comme destination pour le numéro de débogage et le niveau de gravité du message de journal système. Le numéro du message de journal système utilisé est **711001**. Le niveau de gravité par défaut pour ce message de journal système est le débogage.

Étape 5 Cochez la case **Send syslogs in EMBLEM format** (Envoyer les journaux système au format EMBLEM) pour activer le format EMBLEM afin qu'il soit utilisé pour toutes les destinations de journalisation, à l'exception des serveurs de journal système.

Étape 6 Spécifiez la taille du tampon de journal interne dans lequel les messages du journal système sont enregistrés si le tampon de journalisation est activé. Lorsque le tampon est plein, les messages sont remplacés, sauf si vous enregistrez les journaux sur un serveur FTP ou dans la mémoire flash interne. La taille du tampon par défaut est de 4096 octets. La plage va de 4096 à 1048576.

Étape 7 Pour enregistrer le contenu du tampon sur le serveur FTP avant qu'il ne soit remplacé, cochez la case **Save Buffer To FTP Server** (Enregistrer le tampon sur le serveur FTP). Pour autoriser le remplacement du contenu du tampon, décochez cette case.

Étape 8 Cliquez sur **Configure FTP Settings** (Configurer les paramètres FTP) pour identifier le serveur FTP et configurer les paramètres FTP utilisés pour enregistrer le contenu du tampon.

Étape 9 Cochez la case **Save Buffer To Flash** (Enregistrer le tampon dans la mémoire flash) pour enregistrer le contenu du tampon dans la mémoire flash interne avant de le remplacer.



Remarque Cette option est uniquement disponible en mode unique routé ou transparent.

Étape 10 Cliquez sur **Configure Flash Usage** (Configurer l'utilisation de la mémoire flash) pour préciser l'espace maximum à utiliser dans la mémoire flash interne pour la journalisation et l'espace libre minimum à préserver (en Ko). L'activation de cette option crée un répertoire appelé « journal système » sur le disque du périphérique sur lequel les messages sont stockés.



Remarque Cette option est uniquement disponible en mode routé ou transparent unique.

Étape 11 Spécifiez la taille de la file d'attente pour les journaux système qui doivent être consultés dans l'ASA.

Configurer les paramètres FTP

Pour spécifier la configuration du serveur FTP utilisé pour enregistrer le contenu du tampon du journal, procédez comme suit :

Procédure

Étape 1 Cochez la case **Enable FTP client** (Activer le client FTP) pour activer la configuration du client FTP.

Étape 2 Spécifiez l'adresse IP du serveur FTP.

Étape 3 Spécifiez le chemin d'accès au répertoire sur le serveur FTP pour stocker le contenu du tampon du journal enregistré.

Étape 4 Spécifiez le nom d'utilisateur pour vous connecter au serveur FTP.

Étape 5 Spécifiez le mot de passe associé au nom d'utilisateur pour vous connecter au serveur FTP.

Étape 6 Confirmez le mot de passe, puis cliquez sur **OK**.

Configurer l'utilisation de la mémoire flash de journalisation

Pour spécifier les limites d'enregistrement du contenu du tampon de journalisation dans la mémoire flash interne, procédez comme suit :

Procédure

Étape 1 Spécifiez la quantité maximum de mémoire flash interne pouvant être utilisée pour la journalisation (en Ko).

Étape 2 Spécifiez la quantité de mémoire flash interne conservée (en Ko). Lorsque la mémoire flash interne approche cette limite, les nouveaux journaux ne sont plus enregistrés.

Étape 3 Cliquez sur **OK** pour fermer la boîte de dialogue **Configure Logging Flash Usage** (Configurer l'utilisation de la mémoire flash de journalisation).

Activer la journalisation sécurisée

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Server (Serveur de journal système)**.

Étape 2 Sélectionnez un serveur de journal système pour lequel vous souhaitez activer la journalisation sécurisée, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Syslog Server** (Modifier le serveur de journal système) s'affiche.

Étape 3 Cliquez sur le bouton radio **TCP**.

La journalisation sécurisée ne prend pas en charge UDP; une erreur se produit si vous essayez d'utiliser ce protocole.

Étape 4 Cochez la case **Enable secure syslog with SSL/TLS** (Activer le journal système sécurisé avec SSL/TLS), puis cliquez sur **OK**.

Étape 5 (Facultatif) Spécifiez un objet **Reference Identity** (Identité de référence) par nom pour activer les vérifications d'identité de référence RFC 6125 sur le certificat reçu du serveur de journal système.

Consultez Configurer les identités de référence, à la page 828 pour en savoir plus sur l'objet d'identité de référence.

Générer des messages du journal système en format EMBLEM vers un serveur de journal système

Pour générer des messages de journal système au format EMBLEM vers un serveur de journal système, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Server (Serveur de journal système)**.

L'envoi de jounaux système sur IPv6 est pris en charge.

Étape 2 Pour ajouter un nouveau serveur syslog, cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add Syslog Server** (Ajouter un serveur de journal système) s'affiche.



Remarque Vous pouvez configurer un maximum de quatre serveurs de journal système par contexte de sécurité (jusqu'à un total de 16).

Étape 3 Spécifiez le nombre de messages qui peuvent être mis en file d'attente sur l'ASA lorsqu'un serveur de journal système est occupé. Une valeur zéro signifie qu'un nombre illimité de messages peuvent être mis en file d'attente.

Étape 4 Cochez la case **Allow user traffic to pass when TCP syslog server is down** (Autoriser le trafic à passer lorsque le serveur de journal système TCP est en panne) pour autoriser tout le trafic si un serveur de journal système est hors service.

Lorsque l'ASA est configuré pour envoyer des messages de journal système à un serveur de journal système connecté au TCP et si le serveur de journal système tombe en panne, en tant que protection de sécurité, les nouvelles connexions par l'ASA sont bloquées. Pour autoriser de nouvelles connexions, même lorsque le serveur de journal système n'est pas opérationnel, cochez cette case.

Si vous spécifiez UDP, l'ASA continue d'autoriser les nouvelles connexions, que le serveur de journal système soit opérationnel ou non. Les valeurs de port valides sont comprises entre 1025 et 65535, pour l'un ou l'autre de ces protocoles. Le port UDP par défaut est 514. Le port TCP par défaut est 1470.



Remarque L'envoi de journaux système sur TCP n'est pas pris en charge sur un ASA de secours.

Générer des messages du journal système en format EMBLEM vers d'autres destinations de sortie

Pour générer des messages de journal système au format EMBLEM vers d'autres destinations de sortie, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)**.

Étape 2 Cochez la case **Send syslogs in EMBLEM format** (Envoyer les journaux système au format EMBLEM).

Ajouter ou modifier les paramètres du serveur de journal système

Pour ajouter ou modifier les paramètres du serveur de journal système, procédez comme suit :

Procédure

Étape 1 Choisissez l'interface utilisée pour communiquer avec le serveur de journal système dans la liste déroulante.

Étape 2 Saisissez l'adresse IP utilisée pour communiquer avec le serveur de journal système.

Choisissez le protocole (TCP ou UDP) utilisé par le serveur de journal système pour communiquer avec l'ASA ou l'ASASM. Vous pouvez configurer l'ASA et l'ASASM pour envoyer des données à un serveur de journal système en utilisant UDP ou TCP. Le protocole par défaut est UDP si vous n'indiquez pas de protocole.

Avertissement Si vous spécifiez TCP, lorsque l'ASA détecte les défaillances du serveur de journal système, pour des raisons de sécurité, les nouvelles connexions par l'ASA sont bloquées. Pour autoriser de nouvelles connexions malgré les défaillances du serveur de journal système, consultez l'étape 4 de Générer des messages du journal système en format EMBLEM vers un serveur de journal système, à la page 1272.

Étape 3 Saisissez le numéro de port utilisé par le serveur de journal système pour communiquer avec l'ASA ou l'ASASM.

Étape 4 Cochez la case **Log messages in Cisco EMBLEM format (UDP only)** (enregistrer les messages au format Cisco EMBLEM (UDP uniquement)) pour indiquer s'il faut consigner les messages au format Cisco EMBLEM (disponible uniquement si UDP est sélectionné comme protocole).

Étape 5 Cochez la case **Enable secure logging using SSL/TLS (TCP only)** (Activer la journalisation sécurisée à l'aide de SSL/TLS (TCP uniquement)) pour préciser que la connexion au serveur de journal système est sécurisée par l'utilisation de SSL/TLS sur TCP et que le contenu du message de journal système est chiffré. Vous pouvez éventuellement mentionner l'identité de référence pour valider le certificat en fonction de l'objet d'identité de référence précédemment configuré. Pour en savoir plus, consultez Activer la journalisation sécurisée, à la page 1272.

Étape 6 Cliquez sur **OK** pour terminer la configuration.

Envoyer les messages du journal système au tampon du journal interne

Vous devez spécifier quels messages de journal système doivent être envoyés au tampon du journal interne, qui sert d'emplacement de stockage temporaire. Les nouveaux messages sont ajoutés à la fin de la liste. Lorsque le tampon est plein, c'est-à-dire lorsqu'il arrive à saturation, les anciens messages sont remplacés par de nouveaux messages, sauf si vous configurez l'ASA pour enregistrer le tampon complet à un autre emplacement.

Pour envoyer des messages de journal système au tampon du journal interne, procédez comme suit :

Procédure

Étape 1 Choisissez l'une des options suivantes pour spécifier quels messages de journal système doivent être envoyés au tampon du journal interne :

- **Home (Accueil)** > **Latest ASDM Syslog Messages (Derniers messages du journal système ASDM)** > **Configure ASDM Syslog Filters (Configurer les filtres du journal système ASDM)**
- **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**

Étape 2 Choisissez **Monitoring (Supervision)** > **Logging (Journalisation)** > **Log Buffer (Tampon de journal)** > **View (Afficher)**. Sélectionnez ensuite **File (Fichier)** > **Clear Internal Log Buffer (Effacer le tampon du journal interne)** dans le volet **Log Buffer** (Tampon du journal) pour vider le tampon du journal interne.

Étape 3 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)** pour changer la taille du tampon du journal interne. La taille du tampon par défaut est de 4 Ko.

Remarque Lorsque vous modifiez la taille du tampon de journalisation, les journaux existants dans le tampon sont purgés et un nouveau tampon est créé avec la taille nouvellement configurée.

L'ASA continue d'enregistrer les nouveaux messages dans le tampon du journal interne et d'enregistrer le contenu complet de ce tampon dans la mémoire flash interne. Lors de l'enregistrement du contenu du tampon à un autre emplacement, l'ASA crée des fichiers journaux avec des noms qui utilisent le format d'horodatage suivant :

```
LOG-YYYY-MM-DD-HHMMSS.TXT
```

où *AAAA* est l'année, *MM* est le mois, *JJ* est le jour du mois et *HHMMSS* est la durée en heures, minutes et secondes.

Étape 4 Pour enregistrer les nouveaux messages à un autre emplacement, choisissez l'une des options suivantes :

- Cochez la case **Flash** pour envoyer de nouveaux messages à la mémoire flash interne, puis cliquez sur **Configure Flash Usage** (Configurer l'utilisation de la mémoire flash). La boîte de dialogue **Configure Logging Flash Usage** (Configurer l'utilisation de la mémoire flash de journalisation) s'affiche.
  1. Spécifiez la quantité maximum de mémoire flash en Ko que vous souhaitez utiliser pour la journalisation.
  2. Spécifiez la quantité minimum d'espace libre en Ko que la journalisation conservera dans la mémoire flash.
  3. Cliquez sur **OK** pour fermer cette boîte de dialogue.
- Cochez la case **FTP Server** (Serveur FTP) pour envoyer de nouveaux messages à un serveur FTP, puis cliquez sur **Configure FTP Settings** (Configurer les paramètres FTP). La boîte de dialogue **Configure FTP Settings** (Configurer les paramètres FTP) s'affiche.

1. Cochez la case **Enable FTP Client** (Activer le client FTP).
2. Saisissez les renseignements suivants dans les champs fournis : adresse IP du serveur FTP, chemin d'accès, nom d'utilisateur et mot de passe.
3. Confirmez le mot de passe, puis cliquez sur **OK** pour fermer cette boîte de dialogue.

Enregistrer un tampon de journal interne dans la mémoire flash

Pour enregistrer le tampon de journal interne dans la mémoire flash, procédez comme suit :

Procédure

Étape 1 Choisissez **File (Fichier)** > **Save Internal Log Buffer to Flash (Enregistrer le tampon du journal interne dans la mémoire flash)**.

La boîte de dialogue **Enter Log File Name** (Saisir le nom du fichier journal) apparaît.

Étape 2 Choisissez la première option pour enregistrer le tampon du journal avec le nom de fichier par défaut, LOG-YYYY-MM-DD-hhmmss.txt.

Étape 3 Choisissez la deuxième option pour spécifier un nom de fichier pour le tampon du journal.

Étape 4 Saisissez le nom de fichier du tampon du journal, puis cliquez sur **OK**.

Modifier la quantité de mémoire flash interne disponible pour les journaux

Pour modifier la quantité de mémoire flash interne disponible pour les journaux, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)**.

Étape 2 Cochez la case **Enable Logging** (Activer la journalisation).

Étape 3 Cochez la case **Save Buffer to Flash** (Enregistrer le tampon dans la mémoire flash) dans la zone **Logging to Internal Buffer** (Journaliser dans le tampon interne).

Étape 4 Cliquez sur **Configure Flash Usage** (Configurer l'utilisation de la mémoire flash).

La boîte de dialogue **Configure Logging Flash Usage** (Configurer l'utilisation de la mémoire flash de journalisation) s'affiche.

Étape 5 Saisissez la quantité maximum de mémoire flash en Ko autorisée pour la journalisation.

Par défaut, l'ASA peut utiliser jusqu'à 50 Mo de mémoire flash interne pour les données des journaux. La quantité minimum de mémoire flash interne qui doit être libre pour que l'ASA enregistre les données du journal est de 3 Mo. Si un fichier journal enregistré dans la mémoire flash interne entraîne une diminution de l'espace libre dans la mémoire flash interne en dessous de la limite minimum configurée, l'ASA supprime les fichiers journaux les plus anciens afin de garantir qu'il reste suffisamment d'espace libre après

l'enregistrement du nouveau fichier journal. S'il n'y a aucun fichier à supprimer ou si, après la suppression de tous les anciens fichiers, la mémoire libre reste inférieure à la limite, l'ASA ne parvient pas à enregistrer le nouveau fichier journal. La limite maximum de la valeur flash-maximum-allocation est de 2 Go.

Étape 6 Saisissez la quantité minimum d'espace libre en Ko à conserver pour la journalisation dans la mémoire flash.

Étape 7 Cliquez sur **OK** pour fermer la boîte de dialogue **Configure Logging Flash Usage** (Configurer l'utilisation de la mémoire flash de journalisation).

Afficher et copier les entrées enregistrées avec la console Java ASDM

Utilisez la console Java ASDM pour afficher et copier les entrées enregistrées dans un format texte, ce qui peut vous aider à résoudre les erreurs ASDM.

Pour accéder à la console Java ASDM, procédez comme suit :

Procédure

Étape 1 Choisissez **Tools (Outils)** > **ASDM Java Console (Console Java ASDM)**.

Étape 2 Saisissez **m** dans la console pour afficher les statistiques de mémoire de la machine virtuelle.

Étape 3 Saisissez **g** dans la console pour effectuer la collecte des ordures.

Étape 4 Ouvrez le gestionnaire de tâches de Windows et cliquez deux fois sur le fichier **asdm_launcher.exe** pour superviser l'utilisation de la mémoire.

Remarque L'allocation de mémoire maximale autorisée est de 256 Mo.

Envoyer des messages Syslog à une adresse courriel

Pour envoyer des messages de journal système à une adresse courriel, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **E-Mail Setup (Configuration du courriel)**.

Étape 2 Spécifiez l'adresse de courriel utilisée comme adresse source pour les messages syslog envoyés comme courriels.

Étape 3 Cliquez sur **Add** (ajouter) pour saisir la nouvelle adresse de courriel des messages syslog précisés.

Étape 4 Choisissez le niveau de gravité des messages syslog qui sont envoyés au destinataire dans la liste déroulante. Le filtre de gravité des messages syslog utilisé pour l'adresse de courriel de destination entraîne l'envoi des messages du niveau de gravité spécifié et du niveau supérieur. Le filtre global spécifié dans le volet **Logging Filters** (Filtres de journalisation) est également appliqué à chaque destinataire de courriel.

Étape 5 Cliquez sur **Edit** (Modifier) pour modifier un niveau de gravité existant des messages de journal système envoyés à ce destinataire.

Étape 6 Cliquez sur **OK** pour fermer la boîte de dialogue **Add E-mail Recipient** (Ajouter un destinataire de courriel).

Ajouter ou modifier des destinataires de courriel

Pour ajouter ou modifier des destinataires de courriels et des niveaux de gravité, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **E-mail Setup (Configuration du courriel)**.

Étape 2 Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour afficher la boîte de dialogue **Add/Edit E-Mail Recipient** (Ajouter/modifier le destinataire de courriel).

Étape 3 Saisissez l'adresse courriel de destination et choisissez le niveau de gravité du journal système dans la liste déroulante. Les niveaux de gravité sont définis comme suit :

- Urgence (niveau 0, système inutilisable)

Remarque Il est déconseillé d'utiliser le niveau de gravité zéro.

- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Remarque Le niveau de gravité utilisé pour filtrer les messages de l'adresse courriel de destination est le plus élevé entre le niveau de gravité spécifié dans la boîte de dialogue **Add/Edit E-Mail Recipient** (Ajouter/modifier le destinataire de courriel) et le filtre global défini pour tous les destinataires de courriel dans le volet **Logging Filters** (Filtres de journalisation).

Étape 4 Cliquez sur **OK** pour fermer la boîte de dialogue **Add/Edit E-Mail Recipient** (Ajouter/modifier le destinataire de courriel).

L'entrée ajoutée ou révisée apparaît dans le volet **E-mail Recipients** (Destinataires de courriels).

Étape 5 Cliquez sur **Apply** (Appliquer) pour enregistrer vos modifications dans la configuration en cours d'exécution.

Configurer le serveur SMTP distant

Pour configurer le serveur SMTP distant auquel les alertes et les notifications par courriel sont envoyées en réponse à des événements spécifiques, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Logging (Journalisation)** > **SMTP**.

Étape 2 Saisissez l'adresse IP du serveur SMTP principal.

Étape 3 (Facultatif) Saisissez l'adresse IP du serveur SMTP de secours, puis cliquez sur **Apply** (Appliquer) pour enregistrer vos modifications dans la configuration en cours d'exécution.

Envoyer les messages du journal système au port de console

Pour envoyer des messages de journal système au port de console, procédez comme suit :

Procédure

Étape 1 Choisissez une des options suivantes :

- **Home (Accueil)** > **Latest ASDM Syslog Messages (Derniers messages du journal système ASDM)** > **Configure ASDM Syslog Filters (Configurer les filtres du journal système ASDM)**
- **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**

Étape 2 Sélectionnez la console dans la colonne **Logging Destination** (Destination de journalisation), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Logging Filters** (Modifier les filtres de journalisation) s'affiche.

Étape 3 Choisissez des journaux système de toutes les classes d'événements ou des journaux système de classes d'événements spécifiques pour spécifier quels messages de journal système doivent être envoyés au port de console.

Envoyer les messages du journal système à une session Telnet ou SSH

Pour envoyer des messages de journal système à une session Telnet ou SSH, procédez comme suit :

Procédure

Étape 1 Choisissez une des options suivantes :

- **Home (Accueil)** > **Latest ASDM Syslog Messages (Derniers messages du journal système ASDM)** > **Configure ASDM Syslog Filters (Configurer les filtres du journal système ASDM)**
- **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**

Étape 2 Sélectionnez les options **Telnet** et **SSH Sessions** (Sessions SSH) dans la colonne **Logging Destination** (Destination de journalisation), puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Logging Filters** (Modifier les filtres de journalisation) s'affiche.

Étape 3 Choisissez des journaux système de toutes les classes d'événements ou des journaux système de classes d'événements spécifiques pour spécifier quels messages de journal système doivent être envoyés à une session Telnet ou SSH.

Étape 4 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Setup (Configuration de la journalisation)** pour activer la journalisation pour la session en cours uniquement.

Étape 5 Cochez la case **Enable logging** (Activer la journalisation), puis cliquez sur **Apply** (Appliquer).

Configurer les messages du journal système

Configurer la messagerie du journal système

Pour configurer la messagerie du journal système, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration du journal système)**.

Étape 2 Choisissez une fonction de journalisation du système que les serveurs Syslog doivent utiliser comme base pour classer les messages. La valeur par défaut est LOCAL(4)20, ce qui est attendu de la plupart des systèmes UNIX. Cependant, comme vos périphériques réseau partagent huit installations disponibles, vous devrez peut-être modifier cette valeur pour les journaux système.

Étape 3 Cochez la case **Include timestamp in syslogs** (Inclure l'horodatage dans les journaux système) pour ajouter la date et l'heure dans chaque message de journal système envoyé.

Utilisez la liste déroulante **Timestamp Format** (Format d'horodatage) pour sélectionner le format existant (mm:dd:yyyy hh:mm:ss) ou RFC 5424 (yyyy:dd:mmTHH:mm:ssZ).

Étape 4 Décochez la case **Hide username if its validity cannot be determined** (Masquer le nom d'utilisateur si sa validité ne peut pas être déterminée) pour afficher les noms d'utilisateur non valides dans les messages du journal système en cas de tentatives de connexion infructueuses. Le paramètre par défaut consiste à masquer

les noms d'utilisateur lorsque le nom d'utilisateur est non valide ou si la validité est inconnue. Si un utilisateur saisit accidentellement un mot de passe au lieu d'un nom d'utilisateur, par exemple, il est plus sûr de masquer le « nom d'utilisateur » dans le message du journal système résultant. Vous souhaiterez peut-être afficher les noms d'utilisateur non valides pour résoudre les problèmes de connexion.

Étape 5 Choisissez les renseignements à afficher dans le tableau **Syslog ID** (ID de journal système). Les options disponibles sont les suivantes :

- Choisissez **Show all syslog IDs** (Afficher tous les ID du journal système) pour spécifier que le tableau **Syslog ID** (ID du journal système) doit afficher la liste complète des ID des messages du journal système.
- Choisissez **Show disabled syslog IDs** (Afficher les ID de journal système) pour spécifier que le tableau **Syslog ID** (ID de journal système) ne doit afficher que les ID des messages de journal système qui ont été désactivés explicitement.
- Choisissez **Show syslog IDs with changed logging** (Afficher les ID de journal système avec la journalisation modifiée) pour spécifier que le tableau **Syslog ID** (ID de journal système) ne doit afficher que les ID des messages de journal système avec les niveaux de gravité qui ont changé par rapport à leurs valeurs par défaut.
- Choisissez **Show syslog IDs that are disabled or with a changed logging level** (Afficher les ID qui sont désactivés ou avec un niveau de journalisation modifié) pour préciser que le tableau **Syslog ID** (ID de journal système) ne doit afficher que les ID des messages de journal système avec les niveaux de gravité qui ont été modifiés et les ID des messages de journal système qui ont été explicitement désactivés.

Étape 6 Le **Syslog ID Setup Table** (Tableau de configuration d'ID de journal système) affiche la liste des messages de journal système en fonction des paramètres du tableau de configuration d'ID de journal système. Choisissez des messages individuels ou des plages d'ID de message que vous souhaitez modifier. Vous pouvez soit désactiver les ID des messages sélectionnés, soit modifier leurs niveaux de gravité. Pour sélectionner plusieurs ID de message dans la liste, cliquez sur le premier ID de la plage et à l'aide de la touche Maj, cliquez sur le dernier ID de la plage.

Étape 7 Cliquez sur **Advanced** (Avancé) pour configurer les messages du journal système afin d'inclure un ID de périphérique.

Modifier les paramètres d'ID du journal système

Pour modifier les paramètres des messages du journal système, procédez comme suit :



Remarque Le champ **Syslog ID(s)** (ID(s) du journal système) est en lecture seule. Les valeurs qui apparaissent dans cette zone sont déterminées par les entrées que vous avez choisies dans le tableau **Syslog ID** (ID de journal système), situé dans le volet **Syslog Setup** (Configuration du journal système).

Procédure

Étape 1 Cochez la case **Disable Message(s)** (Désactiver le(s) message(s)) pour désactiver les messages correspondant aux ID des messages du journal système affichés dans la liste **Syslog ID(s)** (ID(s) du journal système).

Étape 2 Choisissez le niveau de gravité des messages à envoyer pour les ID des messages du journal système affichés dans la liste **Syslog ID(s)** (ID(s) du journal système). Les niveaux de gravité sont définis comme suit :

- Urgence (niveau 0, système inutilisable)

Remarque Il est déconseillé d'utiliser le niveau de gravité zéro.

- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Étape 3 Cliquez sur **OK** pour fermer la boîte de dialogue **Edit Syslog ID Settings** (Modifier les paramètres d'ID de journal système).

Inclure un ID de périphérique dans les messages du journal système au format non EMBLEM

Pour inclure un ID de périphérique dans les messages du journal système au format non EMBLEM, procédez comme suit :

Procédure

Étape 1 Cochez la case **Enable syslog device ID** (Activer l'ID de périphérique du journal système) pour préciser qu'un ID de périphérique doit être inclus dans tous les messages de journal système au format non EMBLEM.

Étape 2 Pour préciser lequel utiliser comme identifiant de périphérique, choisissez l'une des options suivantes :

- Nom de domaine de l'ASA
- Adresse IP de l'interface

  Choisissez le nom d'interface qui correspond à l'adresse IP sélectionnée dans la liste déroulante.

  Cochez la case **In an ASA cluster, always use control's IP address for the selected interface** (Dans une grappe ASA, toujours utiliser l'adresse IP du contrôle pour l'interface sélectionnée) si vous utilisez la mise en grappe.

- Chaîne

  Spécifiez une chaîne alphanumérique définie par l'utilisateur.

- Nom de la grappe ASA

Étape 3 Cliquez sur **OK** pour fermer la boîte de dialogue **Advanced Syslog Configuration** (Configuration du journal système avancée).

Inclure la date et l'heure dans les messages du journal système

Pour inclure la date et l'heure dans les messages du journal système, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration du journal système)**.

Étape 2 Cochez la case **Include timestamp in syslogs** (Inclure l'horodatage dans les journaux système) dans la zone **Syslog ID Setup** (Configuration de l'ID du journal système).

Étape 3 Cliquez sur **Apply** pour enregistrer vos modifications.

Désactiver un message du journal système

Pour désactiver un message du journal système spécifié, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration du journal système)**.

Étape 2 Sélectionnez le journal système que vous souhaitez désactiver dans le tableau, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Syslog ID Settings** (Modifier les paramètres d'ID du journal système) s'affiche.

Étape 3 Cochez la case **Disable messages** (Désactiver les messages), puis cliquez sur **OK**.

Modifier le niveau de gravité d'un message du journal système

Pour modifier le niveau de gravité d'un message du journal système, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration du journal système)**.

Étape 2 Sélectionnez le journal système dont vous souhaitez modifier le niveau de gravité dans le tableau, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Syslog ID Settings** (Modifier les paramètres d'ID du journal système) s'affiche.

Étape 3 Choisissez le niveau de gravité souhaité dans la liste déroulante **Logging Level** (Niveau de journalisation), puis cliquez sur **OK**.

Bloquer les messages du journal système sur une unité de secours

Pour bloquer la génération de messages de journal système spécifiques sur une unité de secours, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Settings (Paramètres du journal système)**.

Étape 2 Choisissez un ID de journal système dans le tableau, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Syslog ID Settings** (Modifier les paramètres d'ID du journal système) s'affiche.

Étape 3 Cochez la case **Disable messages on standby unit** (Désactiver les messages sur l'unité en veille) pour empêcher la génération des messages du journal système sur une unité en veille.

Étape 4 Cliquez sur **OK** pour fermer cette boîte de dialogue.

Inclure l'ID de périphérique dans les messages du journal système au format non EMBLEM

Pour inclure l'ID de périphérique dans les messages du journal système au format non EMBLEM, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration du journal système)** > **Advanced (Avancé)** > **Advanced Syslog Configuration (Configuration du journal système avancée).**

Étape 2 Cochez la case **Enable syslog device ID** (Activer l'ID de périphérique de journal système).

Étape 3 Cliquez sur le bouton radio **Hostname** (Nom d'hôte), **Interface IP Address** (Adresse IP de l'interface) ou **String** (Chaîne) dans la zone **Device ID** (ID de périphérique).

- Si vous avez choisi l'option **Interface IP Address** (Adresse IP de l'interface), assurez-vous que la bonne interface est sélectionnée dans la liste déroulante.
- Si vous avez choisi l'option **String** (Chaîne), saisissez l'ID de périphérique dans le champ **User-Defined ID** (ID défini par l'utilisateur). La chaîne peut inclure jusqu'à 16 caractères.



Remarque Si cette option est activée, l'ID de périphérique n'apparaît pas dans les messages de journal système au format EMBLEM ni dans les alertes SNMP.

Étape 4 Cliquez sur **OK** pour fermer la boîte de dialogue **Advanced Syslog Configuration** (Configuration du journal système avancée).

Créer une liste d'événements personnalisée

Vous utilisez les trois critères suivants pour définir une liste d'événements :

- Classe d'événement
- Gravité
- ID du message

Pour créer une liste d'événements personnalisé à envoyer à une destination de journalisation spécifique (par exemple, un serveur SNMP), procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Event Lists (Listes d'événements)**.

Étape 2 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Event List** (Ajouter une liste d'événements).

Étape 3 Saisissez le nom de la liste d'événements. Aucun espace n'est autorisé.

Étape 4 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Class and Severity Filter** (Ajouter un filtre de classe et de gravité).

Étape 5 Dans la liste déroulante, choisissez la classe d'événement. Les classes d'événements disponibles varient en fonction du mode de périphérique que vous utilisez.

Étape 6 Choisissez le niveau de gravité dans la liste déroulante. Les niveaux de gravité sont les suivants :

- Urgence (niveau 0, système inutilisable)



Remarque Il est déconseillé d'utiliser le niveau de gravité zéro.

- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Étape 7 Cliquez sur **OK** pour fermer la boîte de dialogue **Add Event List** (Ajouter une liste d'événements).

Étape 8 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Syslog Message ID Filter** (Ajouter un filtre d'ID de message du journal système).

Étape 9 Saisissez un ID de message du journal système ou une plage d'ID (par exemple, 101001-199012) à inclure dans le filtre.

Étape 10 Cliquez sur **OK** pour fermer la boîte de dialogue **Add Event List** (Ajouter une liste d'événements).

L'événement d'intérêt apparaît dans la liste.

Configurer les filtres de journalisation

Appliquer des filtres de message à une destination de journalisation

Pour appliquer des filtres de message à une destination de journalisation, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**.

Étape 2 Choisissez le nom de la destination de journalisation à laquelle vous souhaitez appliquer un filtre. Les destinations de journalisation disponibles sont les suivantes :

- ASDM
- Port de console
- Courriel
- Tampon interne
- Serveur de SNMP
- Serveur journal système
- Session Telnet ou SSH

Cette sélection comprend la deuxième colonne, Journaux système de toutes les classes d'événements, et la troisième colonne, Journaux système de classes d'événements spécifiques. La deuxième colonne répertorie la gravité ou la classe d'événements à utiliser pour filtrer les messages pour la destination de journalisation, ou si la journalisation est désactivée pour toutes les classes d'événements. La troisième colonne répertorie la classe d'événements à utiliser pour filtrer les messages pour cette destination de journalisation.

Étape 3 Cliquez sur **Edit** (Modifier) pour afficher la boîte de dialogue **Edit Logging Filters** (Modifier les filtres de journalisation). Pour appliquer, modifier ou désactiver les filtres, consultez Appliquer des filtres de journalisation, à la page 1287.

Appliquer des filtres de journalisation

Pour appliquer des filtres, procédez comme suit :

Procédure

Étape 1 Choisissez l'option **Filter on severity** (Filtrer par gravité) pour filtrer les messages du journal système en fonction de leur niveau de gravité.

Étape 2 Choisissez l'option **Use event list** (Utiliser la liste d'événements) pour filtrer les messages du journal système en fonction d'une liste d'événements.

Étape 3 Choisissez l'option **Disable logging from all event classes** (Désactiver la journalisation de toutes les classes d'événements) pour désactiver toute la journalisation vers la destination sélectionnée.

Étape 4 Cliquez sur **New** (Nouveau) pour ajouter une nouvelle liste d'événements. Pour ajouter une nouvelle liste d'événements, consultez Créer une liste d'événements personnalisée, à la page 1285.

Étape 5 Dans la liste déroulante, choisissez la classe d'événement. Les classes d'événements disponibles varient en fonction du mode de périphérique que vous utilisez.

Étape 6 Choisissez le niveau de journalisation des messages dans la liste déroulante. Les niveaux de gravité sont les suivants :

- Urgence (niveau 0, système inutilisable)

Remarque Il est déconseillé d'utiliser le niveau de gravité zéro.

- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Étape 7 Cliquez sur **Add** (Ajouter) pour ajouter la classe d'événement et le niveau de gravité, puis cliquez sur **OK**.

La destination de journalisation sélectionnée pour un filtre s'affiche en haut.

Ajouter ou modifier un filtre d'ID de message du journal système

Pour ajouter ou modifier un filtre d'ID de message du journal système, consultez Modifier les paramètres d'ID du journal système, à la page 1281.

Ajouter ou modifier un filtre de classe de message et de gravité

Pour ajouter ou modifier une classe de messages et un niveau de gravité pour le filtrage des messages, procédez comme suit :

Procédure

Étape 1 Dans la liste déroulante, choisissez la classe d'événement. Les classes d'événements disponibles varient en fonction du mode de périphérique que vous utilisez.

Étape 2 Choisissez le niveau de journalisation des messages dans la liste déroulante. Les niveaux de gravité sont les suivants :

- Urgence (niveau 0, système inutilisable)

Remarque Il est déconseillé d'utiliser le niveau de gravité zéro.

- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Étape 3 Cliquez sur **OK** lorsque vous avez terminé vos sélections.

Envoyer tous les messages du journal système d'une classe vers une destination de sortie spécifiée

Pour envoyer tous les messages du journal système d'une classe vers une destination de sortie spécifiée, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**.

Étape 2 Pour remplacer la configuration dans la destination de sortie spécifiée, choisissez la destination de sortie que vous souhaitez modifier, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Logging Filters** (Modifier les filtres de journalisation) s'affiche.

Étape 3 Révisez les paramètres dans la zone **Syslogs from All Event Classes** (Journaux système de toutes les classes d'événements) ou **Syslogs from Specific Event Classes** (Journaux système de classes d'événements spécifiques), puis cliquez sur **OK** pour fermer cette boîte de dialogue.

Par exemple, si vous précisez que les messages de niveau de gravité 7 doivent être envoyés au tampon de journal interne et que les messages de classe ha de niveau de gravité 3 doivent être envoyés au tampon de journal interne, la dernière configuration prévaut.

Pour spécifier qu'une classe doit être envoyée à plusieurs destinations, sélectionnez une option de filtrage différente pour chaque destination de sortie.

Limiter le débit de génération des messages Syslog

Pour limiter le débit de génération des messages du journal système, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Rate Limit (Limite de débit)**.

Étape 2 Choisissez le niveau de journalisation (niveau de gravité du message) auquel vous souhaitez attribuer des limites de débit. Les niveaux de gravité sont définis comme suit :

- Urgence (niveau 0, système inutilisable)
- Alerte (niveau 1, action immédiate requise)
- Critique (niveau 2, conditions critiques)
- Erreur (niveau 3, conditions d'erreur)
- Avertissement (niveau 4, conditions d'avertissement)
- Notification (niveau 5, conditions normales mais significatives)
- Information (niveau 6, messages d'information uniquement)
- Débogage (niveau 7, messages de débogage uniquement)

Étape 3 Le champ **No of Messages** (Nombre de messages) affiche le nombre de messages envoyés. Le champ **Interval (Seconds)** (Intervalle (secondes)) affiche l'intervalle, en secondes, utilisé pour limiter le nombre de messages qui peuvent être envoyés à ce niveau de journalisation. Choisissez un niveau de journalisation dans le tableau et cliquez sur **Edit** (Modifier) pour afficher la boîte de dialogue **Edit Rate Limit for Syslog Logging Level** (Modifier la limite de débit pour le niveau de journalisation système).

Étape 4 Pour continuer, consultez Attribuer ou modifier des limites de débit pour les messages du journal système individuels, à la page 1290.

Attribuer ou modifier des limites de débit pour les messages du journal système individuels

Pour affecter ou modifier des limites de débit à des messages de journal système individuels, procédez comme suit :

Procédure

Étape 1 Pour attribuer la limite de débit d'un message de journal système spécifique, cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Rate Limit for Syslog Message** (Ajouter une limite de débit pour le message de journal système).

Étape 2 Pour continuer, consultez Ajouter ou modifier la limite de débit pour un message du journal système, à la page 1290.

Étape 3 Pour modifier la limite de débit d'un message de journal système spécifique, cliquez sur **Edit** (Modifier) pour afficher la boîte de dialogue **Edit Rate Limit for Syslog Message** (Modifier la limite de débit pour le message de journal système).

Étape 4 Pour continuer, consultez Modifier la limite de débit pour un niveau de gravité du journal système, à la page 1290.

Ajouter ou modifier la limite de débit pour un message du journal système

Pour ajouter ou modifier la limite de débit pour un message de journal système donné, procédez comme suit :

Procédure

Étape 1 Pour ajouter une limite de débit à un message de journal système spécifique, cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Rate Limit for Syslog Message** (Ajouter une limite de débit pour le message de journal système). Pour modifier une limite de débit pour un message de journal système, cliquez sur **Edit** (Modifier) pour afficher la boîte de dialogue **Edit Rate Limit for Syslog Message** (Modifier la limite de débit pour le message de journal système).

Étape 2 Saisissez l'ID de message du journal système que vous souhaitez limiter.

Étape 3 Saisissez le nombre maximum de messages pouvant être envoyés dans l'intervalle de temps spécifié.

Étape 4 Saisissez la durée, en secondes, utilisée pour limiter le débit du message spécifié, puis cliquez sur **OK**.

Remarque Pour autoriser un nombre illimité de messages, laissez les champs **Number of Messages** (Nombre de messages) et **Time Interval** (Intervalle de temps) vides.

Modifier la limite de débit pour un niveau de gravité du journal système

Pour modifier la limite de débit d'un niveau de gravité du journal système spécifié, procédez comme suit :

Procédure

Étape 1 Saisissez le nombre maximum de messages à ce niveau de gravité qui peuvent être envoyés.

Étape 2 Saisissez la durée, en secondes, utilisée pour limiter le débit de messages à ce niveau de gravité, puis cliquez sur **OK**.

Le niveau de gravité des messages sélectionné s'affiche.



Remarque Pour autoriser un nombre illimité de messages, laissez les champs **Number of Messages** (Nombre de messages) et **Time Interval** (Intervalle de temps) vides.

Attribuer ou modifier des limites de débit pour la journalisation dynamique

Vous pouvez attribuer des limites de débit pour la journalisation en fonction des ressources utilisées (taille des blocs). En spécifiant une valeur de seuil (pourcentage), le débit de génération des messages du journal système est limité. Vous pouvez également définir le nombre de messages pouvant être générés lorsque l'utilisation de la taille des blocs dépasse la valeur du seuil.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Rate Limit (Limite de débit)**.

Étape 2 Sous **Rate Limits for Dynamic Logging** (Limites de débit pour la journalisation dynamique), précisez les éléments suivants :

- **Block** (Bloc) : indiquez le pourcentage de blocs libres qui servent de seuil pour déclencher la limitation dynamique du débit.
- **Message Limit (Limite de messages)** : indiquez le nombre de messages autorisés pour la limite dynamique. La valeur par défaut est 10.

Étape 3 Cliquez sur **Apply** (Appliquer).

Étape 4 Pour modifier les valeurs enregistrées, saisissez les nouvelles valeurs, puis cliquez sur **Apply** (Appliquer).

Étape 5 Pour désactiver la limite de débit de journalisation dynamique, laissez les champs vides.

Supervision des journaux

Consultez les commandes suivantes pour superviser l'état de la journalisation.

- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Log Buffer (Tampon de journal)** > **View (Afficher)**

  Ce volet vous permet d'afficher le tampon du journal.

- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Real-Time Log Viewer (Visionneuse de journal en temps réel)** > **View (Afficher)**

  Ce volet vous permet d'afficher le journal en temps réel.

- **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

- **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Critères d'accès)**

  Ce volet vous permet de filtrer la visionneuse en direct de la journalisation de ces journaux en fonction des critères de recherche (ID hexadécimal de la règle). Pour afficher les résultats, sélectionnez la règle et cliquez sur **Show Log** (Afficher le journal).

Filtrer les messages du journal système à l'aide des visionneuses de journaux

Vous pouvez filtrer les messages du journal système en fonction d'une ou plusieurs valeurs correspondant à n'importe quelle colonne de la visionneuse de journal en temps réel et de la visionneuse de tampon de journal.

Pour filtrer les messages du journal système dans l'une des visionneuses de journaux, procédez comme suit :

Procédure

Étape 1 Choisissez une des options suivantes :

- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Real-Time Log Viewer (Visionneuse de journal en temps réel)** > **View (Afficher)**
- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Log Buffer (Tampon de journal)** > **View (Afficher)**

Étape 2 Dans la boîte de dialogue **Real-Time Log Viewer** (Visionneuse de journal en temps réel) ou **Log Buffer Viewer** (Visionneuse de tampon de journal), cliquez sur **Build Filter** (Créer un filtre) dans la barre d'outils.

Étape 3 Dans la boîte de dialogue **Build Filter** (Créer un filtre), spécifiez les critères de filtrage à appliquer aux messages du journal système :

a) Choisissez l'une des trois options suivantes dans la zone **Date and Time** (Date et heure) : en temps réel, heure précise ou plage horaire. Si vous avez choisi une heure précise, indiquez l'heure en saisissant le nombre et en choisissant les heures ou les minutes dans la liste déroulante. Si vous avez choisi une plage horaire, cliquez sur la flèche de la liste déroulante dans le champ **Start Time** (Heure de début) pour afficher un calendrier. Choisissez une date et une heure de début dans la liste déroulante, puis cliquez sur **OK**. Cliquez sur la flèche de la liste déroulante dans le champ **End Time** (Heure de fin) pour afficher un calendrier. Choisissez une date et une heure de fin dans la liste déroulante, puis cliquez sur **OK**.

b) Saisissez un niveau de gravité valide dans le champ **Severity** (Gravité). Vous pouvez également cliquer sur l'icône **Edit** (Modifier) à droite du champ **Severity** (Gravité). Cliquez sur les niveaux de gravité dans la liste que vous souhaitez filtrer. Pour inclure les niveaux de gravité 1 à 7, cliquez sur **All** (Tous). Cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur

l'icône **Info** à droite du champ **Severity** (Gravité) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

c) Saisissez un ID de journal système valide dans le champ **Syslog ID** (ID de journal système). Vous pouvez également cliquer sur l'icône **Edit** (Modifier) à droite du champ **Syslog ID** (ID de journal système). Choisissez une condition de filtrage dans la liste déroulante, puis cliquez sur **Add** (Ajouter). Cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur l'icône **Info** à droite du champ **Syslog ID** (ID de journal système) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

d) Saisissez une adresse IP source valide dans le champ **Source IP Address** (Adresse IP source), ou cliquez sur l'icône **Edit** (Modifier) à droite du champ **Source IP Address** (Adresse IP source). Choisissez une adresse IP unique ou une plage spécifiée d'adresses IP, puis cliquez sur **Add** (Ajouter). Cochez la case **Do not include (exclude) this address or range** (Ne pas inclure (exclure) cette adresse ou cette plage) pour exclure une adresse IP ou une plage d'adresses IP spécifiques, cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur l'icône **Info** à droite du champ **Source IP Address** (Adresse IP source) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

e) Saisissez un port source valide dans le champ **Source Port** (Port source) ou cliquez sur l'icône **Edit** (Modifier) à droite du champ **Source Port** (Port source). Choisissez une condition de filtrage dans la liste déroulante, puis cliquez sur **Add** (Ajouter). Cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur l'icône **Info** à droite du champ **Source Port** (Port source) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

f) Saisissez une adresse IP de destination valide dans le champ **Destination IP Address** (Adresse IP de destination), ou cliquez sur l'icône **Edit** (Modifier) à droite du champ **Destination IP Address** (Adresse IP de destination). Choisissez une adresse IP unique ou une plage spécifiée d'adresses IP, puis cliquez sur **Add** (Ajouter). Cochez la case **Do not include (exclude) this address or range** (Ne pas inclure (exclure) cette adresse ou cette plage) pour exclure une adresse IP ou une plage d'adresses IP spécifiques. Cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur l'icône **Info** à droite du champ **Destination IP Address** (Adresse IP de destination) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

g) Saisissez un port de destination valide dans le champ **Destination Port** (Port de destination) ou cliquez sur l'icône **Edit** (Modifier) à droite du champ **Destination Port** (Port de destination). Choisissez une condition de filtrage dans la liste déroulante, puis cliquez sur **Add** (Ajouter). Cliquez sur **OK** pour afficher ces paramètres dans la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur l'icône **Info** à droite du champ **Destination Port** (Port de destination) pour obtenir des renseignements supplémentaires sur le format d'entrée à utiliser.

h) Saisissez le texte de filtrage dans le champ **Description**. Le texte peut être n'importe quelle chaîne d'un ou plusieurs caractères, y compris une expression régulière. Cependant, les points-virgules ne sont pas des caractères valides et ce paramètre est sensible à la casse. Les entrées multiples doivent être séparées par des virgules.

i) Cliquez sur **OK** pour ajouter les paramètres de filtre que vous venez de spécifier à la liste déroulante **Filter By** (Filtrer par) dans les visionneuses de journaux. Les chaînes de filtre suivent un format spécifique. Le préfixe FILTRE : désigne tous les filtres personnalisés qui apparaissent dans la liste déroulante **Filter By** (Filtrer par). Vous pouvez toujours saisir du texte aléatoire dans ce champ.

Le tableau suivant présente des exemples du format utilisé.

Créer un exemple de filtre	Format de chaîne de filtre
IP source = 192.168.1.1 ou 0.0.0.0 Port source = 67	FILTRE : srcIP=192.168.1.1,0.0.0.0;srcPort=67;

Créer un exemple de filtre	Format de chaîne de filtre
Gravité = informationnelle IP de destination = 1.1.1.1 à 1.1.1.10	FILTRE : sev=6;dstIP=1.1.1.1-1.1.1.10;
ID du journal système non compris entre 725 001 et 725 003	FILTRE : sysID=!725001-725003;
IP source = 1.1.1.1 Description = sortie générée	FILTRE : srcIP=1.1.1.1;descr=sortie générée

Étape 4 Choisissez l'un des paramètres dans la liste déroulante **Filter By** (Filtrer par) pour filtrer les messages du journal système, puis cliquez sur **Filter** (Filtrer) dans la barre d'outils. Ce paramètre s'applique également à tous les futurs messages du journal système. Cliquez sur **Show All** (Afficher tout) dans la barre d'outils pour effacer tous les filtres.

Remarque Vous ne pouvez pas enregistrer des filtres que vous avez spécifiés dans la boîte de dialogue **Build Filter** (Créer un filtre). Ces filtres ne sont valides que pour la session ASDM au cours de laquelle ils ont été créés.

Modifier les paramètres de filtrage

Pour modifier les paramètres de filtrage que vous avez créés à l'aide de la boîte de dialogue **Build Filter** (Créer un filtre), procédez comme suit :

Procédure

Choisissez une des options suivantes :

- Révisez un filtre directement en saisissant les modifications dans la liste déroulante **Filter By** (Filtrer par).
- Choisissez un filtre dans la liste déroulante **Filter By** (Filtrer par), puis cliquez sur **Build Filter** (Créer un filtre) pour afficher la boîte de dialogue **Build Filter** (Créer un filtre). Cliquez sur **Clear Filter** (Effacer le filtre) pour supprimer les paramètres de filtre actuels et en saisir de nouveaux. Sinon, modifiez les paramètres qui s'affichent, puis cliquez sur **OK**.

Remarque Ces paramètres de filtre s'appliquent uniquement à ceux définis dans la boîte de dialogue **Build Filter** (Créer un filtre).

- Cliquez sur **Show All** (Afficher tout) dans la barre d'outils pour arrêter le filtrage et afficher tous les messages du journal système.

Émettre certaines commandes à l'aide des visionneuses de journaux

Vous pouvez exécuter les commandes suivantes à l'aide de l'une des visionneuses de journaux : **ping**, **traceroute**, **whois** et **dns lookup**.

Pour exécuter l'une de ces commandes, procédez comme suit :

Procédure

Étape 1 Choisissez une des options suivantes :

- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Real-Time Log Viewer (Visionneuse de journal en temps réel)** > **View (Afficher)**
- **Monitoring (Supervision)** > **Logging (Journalisation)** > **Log Buffer (Tampon de journal)** > **View (Afficher)**

Étape 2 Cliquez sur **Tools (Outils)** dans le volet **Real-Time Log Viewer** (Visionneuse de journal en temps réel) ou **Log Buffer** (Tampon du journal), puis choisissez la commande que vous souhaitez exécuter. Sinon, vous pouvez cliquer avec le bouton droit sur un message de journal système répertorié pour afficher un menu contextuel, puis choisir la commande que vous souhaitez exécuter.

La boîte de dialogue **Entering command** (Saisie de la commande) s'affiche. La commande que vous avez sélectionnée s'affiche automatiquement dans la liste déroulante.

Étape 3 Saisissez l'adresse IP source ou de destination du message de journal système sélectionné dans le champ **Address** (Adresse), puis cliquez sur **Go** (Aller).

La sortie de la commande s'affiche dans la zone fournie.

Étape 4 Cliquez sur **Clear** (Effacer) pour supprimer la sortie et choisissez une autre commande à exécuter dans la liste déroulante. Répétez l'étape 3, si nécessaire. Cliquez sur **Close** (Fermer) lorsque vous avez terminé.

Historique de journalisation

Tableau 62 : Historique de journalisation

Nom de la caractéristique	Versions de plateforme	Description
Logging (journalisation)	7.0(1)	Fournit des informations de journalisation sur le réseau ASA par le biais de diverses destinations de sortie, et comprend l'option permettant d'afficher et d'enregistrer les fichiers journaux. Nous avons introduit l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Logging Setup (Configuration de la journalisation).
Limite de débit	7.0(4)	Limite le débit auquel les messages de journal système sont générés. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Rate Limit (Limite de débit).
Liste de journalisation	7.2(1)	Crée une liste de journalisation à utiliser dans d'autres commandes pour spécifier les messages selon divers critères (niveau de journalisation, classe d'événement et ID de message). Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Event Lists (Listes d'événements).
Journalisation de sécurité	8.0(2)	Indique que la connexion à l'hôte de journalisation distant doit utiliser SSL/TLS. Cette option est valide uniquement si le protocole sélectionné est TCP. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Server (Serveur de journal système).
Classe de journalisation	8.0(4), 8.1(1)	Ajout de la prise en charge de la classe d'événements ipaa des messages de journalisation. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Logging Filters (Filtres de journalisation).
Classe de journalisation et tampons de journalisation enregistrés	8.2(1)	Ajout de la prise en charge de la classe d'événements dap des messages de journalisation. Ajout de prise en charge pour effacer les tampons de journalisation enregistrés (ASDM, internes, FTP et flash). Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Logging Setup (Configuration de la journalisation).
Chiffrement de mot de passe	8.3(1)	Ajout de la prise en charge du chiffrement de mot de passe.
Visionneuses de journaux	8.3(1)	Les adresses IP sources et de destination ont été ajoutées aux visionneuses de journaux.

Nom de la caractéristique	Versions de plateforme	Description
Journalisation et blocage des connexions améliorés	8.3(2)	Lorsque vous configurez un serveur de journal système pour utiliser TCP et que ce serveur n'est pas disponible, l'ASA bloque les nouvelles connexions qui génèrent des messages de journal système jusqu'à ce que le serveur soit à nouveau disponible (par exemple, les connexions VPN, pare-feu et mandataire direct). Cette fonctionnalité a été améliorée pour bloquer également les nouvelles connexions lorsque la file d'attente de journalisation sur l'ASA est pleine; les connexions reprendront lorsque la file d'attente de journalisation sera effacée. Cette fonctionnalité a été ajoutée pour la conformité aux Common Criteria EAL4+. Sauf si nécessaire, nous avons conseillé d'autoriser les connexions lorsque les messages de journal système ne peuvent pas être envoyés ou reçus. Pour autoriser les connexions, continuez à cochez la case **Allow user traffic to pass when TCP syslog server is down** (Autoriser le trafic utilisateur à passer lorsque le serveur de journal système TCP est en panne) dans le volet Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Servers (Serveurs de journal système). Nous avons introduit les messages de journal système suivants : 414005, 414006, 414007 et 414008. Nous n'avons pas modifié d'écrans ASDM.
Filtrage et tri des messages de journal système	v 8.4(1)	Une prise en charge a été ajoutée pour les éléments suivants : • Filtrage des messages de journal système en fonction de plusieurs chaînes de texte correspondant à différentes colonnes • Création de filtres personnalisés • Tri des messages par colonne. Pour en savoir plus, consultez le guide de configuration ASDM. Cette fonctionnalité est compatible avec toutes les versions d'ASA. Nous avons modifié les écrans suivants : Monitoring (Supervision) > Logging (Journalisation) > Real-Time Log Viewer (Visionneuse de journal en temps réel) > View (Afficher). Monitoring (Supervision) > Logging (Journalisation) > Log Buffer Viewer (Visionneuse de tampon de journal) > View (Afficher).
Mise en grappe	9.0(1)	Ajout de la prise en charge de la génération de messages de journal système dans un environnement de grappe sur l'ASA 5580 et 5585-X. Nous avons modifié l'écran suivant : Configuration > Logging (Journalisation) > Syslog Setup (Configuration du journal système) > Advanced (Avancé) > Advanced Syslog Configuration (Configuration du journal système avancée).

Nom de la caractéristique	Versions de plateforme	Description
Blocage des journaux système sur une unité de secours	9.4(1)	Nous avons ajouté la prise en charge du blocage de la génération de messages de journal système spécifiques sur l'unité de secours dans une configuration de basculement. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Setup (Configuration du journal système).
Identités de référence pour les connexions au serveur de journal système sécurisé	9.6(2)	Le traitement du client TLS prend désormais en charge les règles de vérification de l'identité de serveur définies dans la RFC 6125, section 6. La vérification de l'identité sera effectuée pendant la validation PKI pour les connexions TLS au serveur de journal système. Si l'identité présentée ne correspond pas à l'identité de référence configurée, la connexion n'est pas établie. Nous avons modifié les pages suivantes : **ASDM Configuration (Configuration ASDM) > Remote Access VPN (VPN d'accès à distance) > Advanced (Avancé)** et **Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Servers (Serveurs de journal système) -> Add (Ajouter) ou Edit (Modifier).**
Prise en charge des adresses IPv6 pour les serveurs de journal système	9.7(1)	Vous pouvez maintenant configurer des serveurs de journal système avec des adresses IPv6 pour enregistrer, envoyer et recevoir des journaux système sur TCP et UDP. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Servers (Serveurs de journal système)** > **Add Syslog Server (Ajouter un serveur de journal système)**
Classe de journalisation	9.12(1)	Ajout de la prise en charge de la BFD, du BGP, de l'interface, de l'IPv6, de la multidiffusion, de la commande Object-Group-Search, du PBR, du routage et de la classe SLA des messages de journalisation. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**.
Prise en charge de l'interface de boucle avec retour pour le journal système	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour le journal système. Commandes nouvelles/modifiées : **interface loopback**, **logging host** Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add Loopback Interface (ajouter une interface de bouclage)**. La prise en charge d'ASDM a été ajoutée dans la version 7.19.



CHAPITRE 49

MIB SNMP

Ce chapitre décrit comment configurer le protocole simple de gestion de réseau (SNMP) pour superviser l'ASA.

- À propos de SNMP, à la page 1299
- Lignes directrices pour SNMP, à la page 1302
- Configurer SNMP, à la page 1306
- Supervision SNMP, à la page 1313
- Historique de SNMP, à la page 1314

À propos de SNMP

SNMP est un protocole de couche d'application qui facilite l'échange d'informations de gestion entre les appareils réseau et fait partie de la suite de protocoles TCP /IP. L'ASA prend en charge la surveillance du réseau à l'aide des versions SNMP 1, 2c et 3 de SNMP, et prend en charge l'utilisation des trois versions simultanément. L'agent SNMP qui s'exécute sur l'interface ASA vous permet de surveiller les périphériques réseau à l'aide de systèmes de gestion par réseau (Network Management Systems ou NMS), comme HP OpenView. L'ASA prend en charge l'accès SNMP en lecture seule par l'émission d'une requête GET. L'accès en écriture SNMP n'est pas autorisé, vous ne pouvez donc pas effectuer de modifications avec SNMP. En outre, la requête SNMP SET n'est pas prise en charge.

Vous pouvez configurer la ASA pour envoyer des déroutements, qui sont des messages non sollicités du périphérique géré vers le poste de gestion pour certains événements (notifications d'événement) à un système de gestion de réseau, ou vous pouvez utiliser le système de gestion de réseau pour parcourir les bases d'information de gestion (MIB) sur le périphériques de sécurité. Les MIB sont un ensemble de définitions, et les ASA gèrent une base de données de valeurs pour chaque définition. Parcourir une MIB signifie émettre une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir du système NMS pour déterminer les valeurs.

Remarque Avec des charges de travail intensives, le déploiement de plus de 10 NMS peut avoir une incidence sur les performances de l'appareil. Pour assurer la stabilité et la réactivité de l'appareil, nous vous conseillons d'utiliser avec prudence NMS pour effectuer des interrogations SNMP et gérer le trafic d'interruption.

Les ASA possèdent un agent SNMP qui informe les stations de gestion désignées si des événements prédéfinis nécessitent une notification, par exemple, lorsqu'une liaison du réseau monte ou tombe en panne. La notification

qu'il envoie comprend un OID SNMP, qui s'identifie aux stations de gestion. L'agent ASA répond également lorsqu'une station de gestion demande des renseignements.

Terminologie SNMP

Le tableau suivant répertorie les termes couramment utilisés avec SNMP.

Tableau 63 : Terminologie SNMP

Terme	Description
Agent	Le serveur SNMP exécuté sur ASA. L'agent SNMP présente les caractéristiques suivantes : • Répond aux demandes d'informations et d'actions du poste de gestion de réseau. • Contrôle l'accès à sa base d'information de gestion, l'ensemble d'objets que le gestionnaire SNMP peut afficher ou modifier. • N'autorise pas les opérations SET.
Navigation	Surveille l'intégrité d'un périphérique à partir du poste de gestion de réseau en interrogeant les informations requises de l'agent SNMP sur le périphérique. Cette activité peut comprendre l'émission d'une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir du poste de gestion de réseau afin de déterminer les valeurs.
Bases d'informations de gestion (MIB)	Structures de données normalisées pour la collecte d'informations sur les paquets, les connexions, les tampons, les basculements, etc. Les MIB sont définies par le produit, les protocoles et les normes matérielles utilisés par la plupart des périphériques réseau. Les stations de gestion de réseau SNMP peuvent parcourir les MIB et demander l'envoi de données ou d'événements précis au fur et à mesure qu'ils se produisent.
Postes de gestion de réseau (NSM, Network Management Station)	Les ordinateurs ou postes de travail configurés pour superviser les événements SNMP et gérer les périphériques, tels que l'ASA
Identifiant d'objet (OID)	Le système qui identifie un appareil auprès de son système de gestion système et indique aux utilisateurs la source des renseignements surveillés et affichés.
Trap	Événements prédéfinis qui génèrent un message de l'agent SNMP au système NMS. Les événements comprennent des conditions d'alarme telles qu'un démarrage, un retrait, un démarrage à froid, un démarrage à chaud, une authentification ou des messages syslog.

Présentation du SNMP version 3

SNMP version 3 offre des améliorations de sécurité qui ne sont pas disponibles dans les versions SNMP 1 et 2c. Les versions SNMP 1 et 2c transmettent des données entre le serveur SNMP et l'agent SNMP en texte clair. SNMP version 3 ajoute des options d'authentification et de confidentialité pour sécuriser les opérations du protocole. En outre, cette version contrôle l'accès à l'agent SNMP et aux objets MIB par le biais du modèle de sécurité basé sur l'utilisateur (USM) et du modèle de contrôle d'accès basé sur l'affichage (VACM). L'ASA prend également en charge la création de groupes SNMP et d'utilisateurs, ainsi que d'hôtes, ce qui est nécessaire pour activer l'authentification et le chiffrement du transport pour des communications SNMP sécurisées.

Modèles de sécurité

À des fins de configuration, les options d'authentification et de confidentialité sont regroupées dans des modèles de sécurité. Les modèles de sécurité s'appliquent aux utilisateurs et aux groupes, qui sont répartis dans les trois types suivants :

- NoAuthPriv : pas d'authentification ni de confidentialité, ce qui signifie qu'aucune sécurité n'est appliquée aux messages.
- AuthNoPriv : authentification mais pas de confidentialité, ce qui signifie que les messages sont authentifiés.
- AuthPriv : authentification et confidentialité, ce qui signifie que les messages sont authentifiés et chiffrés.

SNMP Groups (groupes SNMP)

Un groupe SNMP est une stratégie de contrôle d'accès à laquelle des utilisateurs peuvent être ajoutés. Chaque groupe SNMP est configuré avec un modèle de sécurité et est associé à une vue SNMP. Un utilisateur appartenant à un groupe SNMP doit correspondre au modèle de sécurité du groupe SNMP. Ces paramètres spécifient le type d'authentification et de confidentialité utilisé par un utilisateur appartenant à un groupe SNMP. Chaque paire de noms de groupes SNMP et de modèles de sécurité doit être unique.

Utilisateurs SNMP

Les utilisateurs SNMP disposent d'un nom d'utilisateur spécifié, d'un groupe auquel ils appartiennent, d'un mot de passe d'authentification, d'un mot de passe de chiffrement et d'algorithmes d'authentification et de chiffrement à utiliser. Les options d'algorithme d'authentification sont SHA-1, SHA-224, SHA-256 HMAC et SHA-384. Les options d'algorithme de chiffrement sont 3DES et AES (qui sont disponibles en versions 128, 192 et 256). Lorsque vous créez un utilisateur, vous devez l'associer à un groupe SNMP. L'utilisateur hérite ensuite du modèle de sécurité du groupe.



Remarque Lors de la configuration d'un compte d'utilisateur SNMPv3, assurez-vous que la longueur de l'algorithme d'authentification est égale ou supérieure à la longueur de l'algorithme de chiffrement.

Hôtes SNMP

Un hôte SNMP est une adresse IP à laquelle les notifications et les alertes SNMP sont envoyées. Pour configurer les hôtes SNMP version 3, ainsi que l'adresse IP cible, vous devez configurer un nom d'utilisateur, car les alertes ne sont envoyées qu'à un utilisateur configuré. Les adresses IP cibles SNMP et les noms de paramètre cibles doivent être uniques sur l'ASA. Chaque hôte SNMP ne peut être associé qu'à un seul nom d'utilisateur. Pour recevoir des alertes SNMP, configurez le NMS SNMP et assurez-vous de configurer les renseignements d'authentification de l'utilisateur sur le NMS pour qu'ils correspondent aux renseignements d'authentification de l'ASA.



Remarque Vous pouvez ajouter jusqu'à 8 192 hôtes. Cependant, seulement 128 de ceux-ci peuvent être utilisés pour les déroutements.

Différences d'implémentation entre les logiciels ASA et Cisco IOS

La mise en œuvre de SNMP version 3 dans l'ASA diffère de la mise en œuvre de SNMP version 3 dans le logiciel Cisco IOS de la manière suivante :

- Les ID du moteur local et du moteur distant ne sont pas configurables. L'ID du moteur local est généré au démarrage de l'ASA ou lors de la création d'un contexte.
- Aucune prise en charge n'existe pour le contrôle d'accès basé sur l'affichage, ce qui entraîne une navigation MIB non limitée.
- La prise en charge est limitée aux MIB suivantes : USM, VACM, FRAMEWORK et TARGET.
- Vous devez créer des utilisateurs et des groupes avec le modèle de sécurité approprié.
- Vous devez supprimer les utilisateurs, les groupes et les hôtes dans le bon ordre.
- L'utilisation de la commande snmp-server host crée une règle ASA pour autoriser le trafic SNMP entrant.

Messagerie du journal système SNMP

SNMP génère des messages de journal système détaillés, numérotés 212*nnn*. Les messages du journal système indiquent l'état des requêtes SNMP, des interruptions SNMP, des canaux SNMP et des réponses SNMP de l'ASA ou de l'ASASM à un hôte spécifié sur une interface spécifiée.

Pour obtenir des renseignements détaillés sur les messages du journal système, consultez le guide des messages de journal système.

Remarque L'interrogation SNMP échoue si les messages de journal système du protocole SNMP dépassent un débit élevé (environ 4 000 par seconde).

Services d'application et outils tiers

Pour en savoir plus sur la prise en charge de SNMP, consultez l'URL suivante :

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

Pour en savoir plus, consultez le chapitre SNMP du Guide de configuration d'ASDM pour les opérations générales Cisco ASA à l'URL suivante :

https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html

Lignes directrices pour SNMP

Cette section comprend les lignes directrices et les limites que vous devez consulter avant de configurer SNMP.

Lignes directrices en matière de basculement et de mise en grappe

- Lorsque vous utilisez SNMPv3 avec mise en grappe ou basculement, si vous ajoutez une nouvelle unité de grappe après la formation initiale de la grappe ou si vous remplacez une unité de basculement, les utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez rajouter les utilisateurs SNMPv3 à l'unité de contrôle ou active pour forcer les utilisateurs à être dupliqués sur la nouvelle unité; ou vous pouvez ajouter les utilisateurs directement sur la nouvelle unité (les utilisateurs et les groupes SNMPv3 sont une exception à la règle selon laquelle vous ne pouvez pas saisir de commandes de configuration sur une unité de données en grappe). Reconfigurez chaque utilisateur en saisissant la commande **snmp-server user** *username group-name* **v3** sur l'unité de contrôle/active ou directement sur l'unité de données/secours avec les options *priv-password* et *auth-password* dans leur format non chiffré.

Lignes directrices relatives à IPv6 (tous les modèles ASA)

SNMP peut être configuré sur le transport IPv6 de sorte qu'un hôte IPv6 puisse exécuter des requêtes SNMP et recevoir des notifications SNMP d'un périphérique exécutant le logiciel IPv6. L'agent SNMP et les MIB associées ont été améliorés pour prendre en charge l'adressage IPv6.

Lignes directrices relatives à IPv6 pour Firepower 2100

Firepower 2100 exécute un système d'exploitation sous-jacent appelé FXOS et prend en charge le mode appareil (par défaut) et le mode plateforme; voir Régler le Firepower 2100 en mode appareil ou plateforme, à la page 47.

En mode plateforme, vous devez configurer une adresse IP de gestion IPv6 dans FXOS. Dans l'exemple suivant, une passerelle et une interface de gestion IPv6 sont configurées :

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
Management IPv6 Interface:
IPv6 Address Prefix IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998 64 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

Directives supplémentaires

- Les interruptions d'alimentation ne sont pas émises pour les systèmes fonctionnant en mode appareil.
- Pour Firepower 2100, en mode plateforme, vous ne pouvez pas interroger les interfaces membres d'un EtherChannel, et les interruptions pour les interfaces membres ne sont pas générées. Cette fonctionnalité est prise en charge si vous activez SNMP directement dans FXOS. Le mode appareil n'est pas affecté.
- Ne prend pas en charge les interruptions ASA pour les membres de ports individuels pour le Firepower 2100 en mode plateforme; consultez le Guide de référence de Cisco Firepower 2100 FXOS MIB.
- Pour Firepower 2100, en mode appareil, vous ne pouvez pas interroger le modèle matériel ni le numéro de série. De plus, dans l'ASA, les interruptions ne sont pas générées pour ces détails. Par conséquent,

configurez SNMP sur FXOS ou Chassis Manager pour interroger l'adresse IP de gestion de châssis au lieu des interfaces sur l'instance ASA.

- Vous devez disposer de Cisco Works pour Windows ou d'un autre navigateur conforme à SNMP MIB-II pour recevoir des alertes SNMP ou parcourir une MIB.
- L'accès de gestion sur un tunnel VPN n'est pas pris en charge avec SNMP (la commande **management-access**). Pour SNMP sur VPN, nous vous recommandons d'activer SNMP sur une interface de boucle avec retour. Vous n'avez pas besoin d'activer la fonctionnalité d'accès de gestion pour utiliser SNMP sur l'interface de boucle avec retour. La boucle avec retour fonctionne également pour SSH.
- Ne prend pas en charge le contrôle d'accès basé sur l'affichage, mais il est possible de parcourir la MIB VACM pour déterminer les paramètres d'affichage par défaut.
- ENTITY-MIB n'est pas disponible dans le contexte de non-administration. Utilisez plutôt IF-MIB pour effectuer des requêtes dans le contexte de non-administration.
- ENTITY-MIB n'est pas disponible pour le Firepower 9300. Utilisez plutôt CISCO-FIREPOWER-EQUIPMENT-MIB et CISCO-FIREPOWER-SM-MIB.
- Sur certains périphériques, il a été observé que l'ordre des interfaces (ifDescr) dans la sortie de **snmpwalk** change après un redémarrage. L'ASA utilise un algorithme pour déterminer le tableau ifIndex que SNMP interroge. Lorsque l'ASA est démarré, les interfaces sont ajoutées au tableau ifIndex dans l'ordre chargé au fur et à mesure que l'ASA lit la configuration. Les nouvelles interfaces ajoutées à l'ASA sont ajoutées à la liste des interfaces dans le tableau ifIndex. Lorsque des interfaces sont ajoutées, supprimées ou renommées, cela peut affecter l'ordre des interfaces lors du redémarrage.
- Lorsque vous fournissez un OID dans la commande **snmpwalk**, l'outil snmpwalk interroge toutes les variables de la sous-arborescence qui se trouve sous l'OID spécifié et affiche leurs valeurs. Ainsi, pour afficher une sortie complète des objets sur le périphérique, assurez-vous de fournir l'OID dans la commande **snmpwalk**.
- Ne prend pas en charge la version 3 du SNMP pour AIP SSM ou AIP SSC.
- Ne prend pas en charge le débogage SNMP.
- Ne prend pas en charge la récupération des renseignements ARP.
- Ne prend pas en charge les commandes SNMP NET.
- Lorsque vous utilisez NET-SNMP version 5.4.2.1, prend uniquement en charge la version de l'algorithme de chiffrement AES128. Ne prend pas en charge les versions des algorithmes de chiffrement AES256 ou AES192.
- Les modifications apportées à la configuration existante sont refusées si le résultat place la fonctionnalité SNMP dans un état incohérent.
- Pour la version 3 de SNMP, la configuration doit avoir lieu dans l'ordre suivant : groupe, utilisateur, hôte.
- Pour Firepower 2100, lorsque SNMPv3 est configuré sur l'interface de gestion des périphériques, tous les utilisateurs de SNMPv3 peuvent interroger le périphérique même lorsqu'ils ne sont pas mappés dans la configuration de l'hôte.
- Pour les modèles Secure Firewall, la commande **snmpwalk** interroge les membres FXOS uniquement à partir du contexte d'administration.

- Avant de supprimer un groupe, vous devez vous assurer que tous les utilisateurs associés à ce groupe sont supprimés.
- Avant de supprimer un utilisateur, vous devez vous assurer qu'aucun hôte associé à ce nom d'utilisateur n'est configuré.
- Si les utilisateurs ont été configurés pour appartenir à un groupe particulier avec un certain modèle de sécurité, et si le niveau de sécurité de ce groupe est modifié, vous devez effectuer les opérations suivantes dans cet ordre :
  - Supprimer les utilisateurs de ce groupe.
  - Modifier le niveau de sécurité du groupe.
  - Ajouter des utilisateurs qui appartiennent au nouveau groupe.
- La création de vues personnalisées pour restreindre l'accès des utilisateurs à un sous-ensemble d'objets MIB n'est pas prise en charge.
- Toutes les requêtes et toutes les interruptions sont disponibles uniquement dans la vue Lecture/Notification par défaut.
- L'interruption de la limite de connexion atteinte est générée dans le contexte d'administration. Pour générer cette interruption, vous devez avoir au moins un hôte de serveur SNMP configuré dans le contexte d'utilisateur dans lequel la limite de connexion a été atteinte.
- Si le NMS ne parvient pas à demander des objets avec succès ou ne gère pas correctement les interruptions entrantes de l'ASA, la capture de paquets est la méthode la plus utile pour déterminer le problème. Choisissez **Wizards (Assistants) > Packet Capture Wizard (Assistant de capture de paquets)** et suivez les instructions à l'écran.
- Vous pouvez ajouter jusqu'à 4 000 hôtes. Cependant, seulement 128 de ceux-ci peuvent être utilisés pour les déroutements.
- Le nombre total de destinations d'interrogation actives prises en charge est de 128.
- Vous pouvez spécifier un objet réseau pour indiquer les hôtes individuels que vous souhaitez ajouter en tant que groupe d'hôtes.
- Vous pouvez associer plusieurs utilisateurs à un hôte.
- Vous pouvez spécifier des objets réseau qui se chevauchent dans différentes commandes **host-group**. Les valeurs que vous spécifiez pour le dernier groupe d'hôtes s'appliquent à l'ensemble commun d'hôtes dans les différents objets réseau.
- Si vous supprimez un groupe d'hôtes ou des hôtes qui se chevauchent avec d'autres groupes d'hôtes, les hôtes sont reconfigurés en utilisant les valeurs qui ont été spécifiées dans les groupes d'hôtes configurés.
- Les valeurs acquises par les hôtes dépendent de la séquence spécifiée que vous utilisez pour exécuter les commandes.
- La limite de taille des messages que SNMP envoie est de 1 472 octets.
- L'ASA prend en charge un nombre illimité d'hôtes d'interruption de serveur SNMP par contexte. La sortie de la commande **show snmp-server host** affiche uniquement les hôtes actifs qui interrogent l'ASA, ainsi que les hôtes configurés de manière statique.

Configurer SNMP

Cette section décrit comment configurer SNMP.

Procédure

Étape 1 Configurez une station de gestion SNMP pour recevoir les demandes de l'ASA.

Étape 2 Configurez les alertes SNMP.

Étape 3 Configurez les paramètres SNMP de version 1 et 2c ou les paramètres SNMP de version 3.

Configurer une station de gestion SNMP

Pour configurer une station de gestion SNMP, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP**. Par défaut, le serveur SNMP est activé.

Étape 2 Cliquez sur **Add** (Ajouter) dans le volet **SNMP Management Stations** (Stations de gestion SNMP).

La boîte de dialogue **Add SNMP Host Access Entry** (Ajouter une entrée d'accès à l'hôte SNMP) s'affiche.

Étape 3 Choisissez l'interface sur laquelle se trouve l'hôte SNMP.

Étape 4 Entrez l'adresse IP de l'hôte SNMP.

Étape 5 Saisissez le port UDP de l'hôte SNMP ou conservez la valeur par défaut, le port 162.

Étape 6 Ajoutez l'identifiant de communauté de l'hôte SNMP. Si aucun identifiant de communauté n'est précisé pour une station de gestion, la valeur définie dans le champ **Community String** (Identifiant de communauté) (par défaut) du volet **SNMP Management Stations** (Stations de gestion SNMP) est utilisée.

Étape 7 Choisissez la version SNMP utilisée par l'hôte SNMP.

Étape 8 Si vous avez sélectionné la version 3 du SNMP à l'étape précédente, choisissez le nom d'un utilisateur configuré.

Étape 9 Pour spécifier la méthode de communication avec ce NMS, cochez la case **Poll** (Interrogation) ou **Trap** (Interruption).

Étape 10 Cliquez sur **OK**.

La boîte de dialogue **Add SNMP Host Access Entry** (Ajouter une entrée d'accès à l'hôte SNMP) se ferme.

Étape 11 Cliquez sur **Apply** (Appliquer).

Le NMS est configuré et les modifications sont enregistrées dans la configuration en cours d'exécution. Pour en savoir plus, consultez le chapitre SNMP du Guide de configuration d'ASDM pour les opérations générales Cisco ASA à l'URL suivante :

https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html

Configurer les déroutements SNMP

Pour désigner les interruptions que l'agent SNMP génère et la manière dont elles sont collectées et envoyées aux NMS, procédez comme suit :

Remarque Lorsque vous activez toutes les alertes de SNMP ou de syslog, il est possible que le processus SNMP consomme les ressources excédentaires de l'agent et du réseau, ce qui entraîne le blocage du système. Si vous remarquez des retards du système, des demandes non terminées ou des échéances de délais d'expiration, vous pouvez activer de manière sélective les déroutements SNMP et syslog. Par exemple, vous pouvez ignorer le niveau de gravité *Informational* (Informationnel) de l'interruption de journal système.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP**.

Étape 2 Cliquez sur **Configure Traps** (Configurer les interruptions).

La boîte de dialogue **SNMP Trap Configuration** (Configuration de l'interruption SNMP) s'affiche.

Étape 3 Cochez la case **SNMP Server traps configuration** (Configuration des interruptions de serveur SNMP).

Toutes les interruptions standard SNMP sont activées dans la configuration par défaut. Si vous ne spécifiez pas de type d'interruption, la valeur par défaut est l'interruption **syslog** (journal système). Les alertes SNMP par défaut continuent d'être activées avec l'interruption **syslog** (journal système). Toutes les autres interruptions sont désactivées par défaut. Pour désactiver une interruption, décochez la case applicable.

Les interruptions sont classées dans les catégories suivantes :

a) **Standard SNMP Traps** (Alertes SNMP standard), cochez tout ce qui s'applique.

Choisissez parmi **Critical CPU temperature** (Température du CPU critique), **Chassis temperature** (Température du châssis), et **Chassis Fan Failure** (Défaillance du ventilateur du châssis).

Remarque Toutes les interruptions standard SNMP sont activées dans la configuration par défaut.

b) **Environment Traps** (Interruptions d'environnement), cochez tout ce qui s'applique.

Choisissez parmi **Authentication** (Authentification), **Link up** (Reconnexion), **Link down** (Déconnexion), **Cold start** (Démarrage à froid) et **Warm start** (Démarrage à chaud).

c) **Ikev2 Traps** (Interruptions Ikev2), cochez tout ce qui s'applique.

Choisissez parmi **Start** (Démarrer) et **Stop** (Arrêter).

d) **Entity MIB Notifications** (Notifications MIB de l'entité).

Cochez cet élément pour recevoir des notifications sur les unités remplaçables sur site.

e) **IPsec Traps** (Interruptions IPsec), cochez tout ce qui s'applique.

Choisissez parmi **Start** (Démarrer) et **Stop** (Arrêter).

f) **Remote Access Traps** (Interruptions d'accès à distance).

Cochez cet élément pour recevoir des notifications lorsque le nombre de sessions établies dépasse le seuil défini.

g) **Resource Traps** (Interruptions de ressources), cochez tout ce qui s'applique.

Choisissez parmi **Connection limit reached** (Limite de connexion atteinte), **Memory threshold reached** (Seuil de mémoire atteint) et **Interface threshold reached** (Seuil d'interface atteint).

h) **NAT Traps** (Interruptions NAT).

Cochez cet élément pour recevoir des notifications lorsque des paquets IP sont rejetés par la NAT en raison de l'espace de mappage non disponible.

i) **Syslog** (Journal système).

Cochez **Enable syslog traps** (Activer les interruptions du journal système) pour recevoir des notifications lorsque le nombre de sessions établies dépasse le seuil défini.

Pour configurer le niveau de gravité de l'interruption **syslog** (journal système), sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Logging Filters (Filtres de journalisation)**

j) **CPU Utilization Traps** (Interruptions d'utilisation du CPU).

Cochez **CPU rising threshold reached** (Seuil d'augmentation du CPU atteint) pour recevoir des notifications lorsque l'utilisation du CPU est supérieure à la valeur **CPU Utilization threshold** (Seuil d'utilisation du CPU) configurée pour la valeur **Monitoring interval** (Intervalle de supervision) configurée.

k) **SNMP interface threshold** (Seuil d'interface SNMP).

Cochez **Configure threshold and interval** (Configurer le seuil et l'intervalle) pour recevoir des notifications lorsque l'utilisation de la bande passante de l'interface est supérieure à la valeur **SNMP interface threshold** (Seuil d'interface SNMP) configurée.

Les valeurs de seuil valides sont comprises entre 30 et 99 %. La valeur par défaut est 70 %.

l) **SNMP Memory threshold** (Seuil de mémoire SNMP).

Cochez **Configure memory threshold** (Configurer le seuil de mémoire) pour recevoir des notifications lorsque l'utilisation du CPU est supérieure à la valeur de seuil configurée pour la valeur **SNMP memory threshold** (Seuil de mémoire SNMP).

Lorsque la mémoire du contexte système utilisée atteint 80 % de la mémoire totale du système, l'interruption de seuil de mémoire est générée à partir du contexte d'administration. Pour tous les autres contextes d'utilisateur, cette interruption est générée lorsque la mémoire utilisée atteint 80 % de la mémoire totale du système dans ce contexte en particulier.

m) **Failover Traps** (Interruptions de basculement).

Cochez **Enable Failover related traps** (Activer les interruptions liées au basculement) pour recevoir les alertes SNMP du journal système pour le basculement.

n) **Cluster Traps** (Interruptions de grappe).

Cochez **Enable cluster related traps** (Activer les interruptions liées à la grappe) pour recevoir les alertes SNMP du journal système pour les membres de la grappe.

o) **Peer-Flap Traps** (Interruptions d'intermittence d'homologues).

Cochez **Enable bgp/ospf peer-flap related traps** (Activer les interruptions d'intermittence d'homologues BGP/OSPF) pour recevoir les alertes SNMP du journal système pour le basculement involontaire des adresses MAC des homologues de grappe.

Étape 4 Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du déroutement SNMP**.

Étape 5 Cliquez sur **Apply** (Appliquer).

Les alertes SNMP sont configurées et les modifications sont enregistrées dans la configuration en cours d'exécution.

Configurer les paramètres pour la version 1 ou 2c du SNMP

Pour configurer les paramètres pour la version 1 ou 2c du SNMP, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP** .

Étape 2 Saisissez un identifiant de communauté par défaut dans le champ **Community String** (Identifiant de communauté) (par défaut) si vous utilisez la version 1 ou 2c du SNMP. Saisissez le mot de passe utilisé par les NMS SNMP lorsqu'ils envoient des requêtes à l'ASA. L'identifiant de communauté SNMP est un secret partagé entre les NMS SNMP et les nœuds de réseau gérés. L'ASA utilise le mot de passe pour déterminer si la requête SNMP entrante est valide. Cependant, si la supervision SNMP se fait par l'interface de gestion plutôt que par l'interface de diagnostic, l'interrogation a lieu sans que l'ASA ne valide l'identifiant de communauté. Le mot de passe est une valeur sensible à la casse pouvant comporter jusqu'à 32 caractères alphanumériques. Les espaces ne sont pas permises. La valeur par défaut est public. La version 2c du SNMP permet de définir des identifiants de communauté distincts pour chaque NMS. Si aucun identifiant de communauté n'est configuré pour un NMS, la valeur définie ici est utilisée par défaut.

Remarque Vous devez éviter l'utilisation de caractères spéciaux (!, @, #, $, %, ^, &, *, \) dans les identifiants de communauté. En général, l'utilisation de caractères spéciaux réservés aux fonctions utilisées par le système d'exploitation peut entraîner des résultats inattendus. Par exemple, la barre oblique inverse (\) est interprétée comme un caractère d'échappement et ne doit pas être utilisée dans l'identifiant de communauté.

Étape 3 Saisissez le nom de l'administrateur système de l'ASA. Le texte est sensible à la casse et peut comporter jusqu'à 127 caractères alphabétiques. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.

Étape 4 Saisissez l'emplacement de l'ASA géré par SNMP. Le texte est sensible à la casse et peut comporter jusqu'à 127 caractères. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.

Étape 5 Saisissez le numéro de port de l'ASA qui écoute les requêtes SNMP à partir des NMS; ou conservez la valeur par défaut, le numéro de port 161.

Étape 6 (Facultatif) Cochez la case **Enable Global-Shared pool in the walk** (Activer le groupe partagé global dans la marche) pour interroger la mémoire libre et les statistiques de mémoire utilisées au moyen des opérations de marche SNMP.



Important Lorsque l'ASA interroge les renseignements sur la mémoire, le CPU peut être occupé par le processus SNMP pendant trop longtemps avant d'être libéré pour d'autres processus. Cela peut entraîner des saturations du CPU liées à SNMP qui peuvent entraîner des abandons de paquet.

Étape 7 Cliquez sur **Add** (Ajouter) dans le volet **SNMP Host Access List** (Liste d'accès de l'hôte SNMP).

La boîte de dialogue **Add SNMP Host Access Entry** (Ajouter une entrée d'accès à l'hôte SNMP) s'affiche.

Étape 8 Choisissez le nom de l'interface à partir de laquelle les interruptions sont envoyées dans la liste déroulante.

Étape 9 Saisissez l'adresse IP du gestionnaire NMS ou SNMP qui peut se connecter à l'ASA.

Étape 10 Saisissez le numéro de port UDP. La valeur par défaut est 162.

Étape 11 Choisissez la version SNMP que vous utilisez dans la liste déroulante. Si vous choisissez la version 1 ou la version 2c, vous devez saisir l'identifiant de communauté. Si vous choisissez la version 3, vous devez choisir le nom d'utilisateur dans la liste déroulante.

La version spécifie la version du SNMP à utiliser pour les interruptions et les requêtes (interrogation). La communication avec le serveur est autorisée uniquement en utilisant la version sélectionnée.

Étape 12 Cochez la case **Poll** (Interrogation) dans la zone **Server Poll/Trap Specification** (Spécification de l'interrogation et de l'interruption du serveur) pour limiter le NMS à l'envoi de requêtes (interrogation). Cochez la case **Trap** (Interruption) pour limiter le NMS à la réception d'interruptions uniquement. Vous pouvez cocher les deux cases pour effectuer les deux fonctions de l'hôte SNMP.

Étape 13 Cliquez sur **OK** pour fermer la boîte de dialogue **Add SNMP Host Access Entry** (Ajouter une entrée d'accès à l'hôte SNMP).

Le nouvel hôte apparaît dans le volet **SNMP Host Access List** (Liste d'accès à l'hôte SNMP).

Étape 14 Cliquez sur **Apply**.

Les paramètres SNMP pour les versions 1, 2c ou 3 sont configurés et les modifications sont enregistrées dans la configuration en cours d'exécution.

Configurer les paramètres pour la version 3 du SNMP

Pour configurer les paramètres pour la version 3 du SNMP, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP**.

Étape 2 Cliquez sur **Add (Ajouter)** > **SNMP User (Utilisateur SNMP)** sous l'onglet **SNMPv3 User/Group** (Utilisateur/Groupe SNMPv3) dans le volet **SNMPv3 Users** (Utilisateurs SNMPv3) pour ajouter un utilisateur configuré ou un nouvel utilisateur à un groupe. Lorsque vous supprimez le dernier utilisateur d'un groupe, ASDM supprime le groupe.

Remarque Après la création d'un utilisateur, vous ne pouvez pas modifier le groupe auquel appartient l'utilisateur.

La boîte de dialogue **Add SNMP User Entry** (Ajouter une entrée d'utilisateur SNMP) s'affiche.

Étape 3 Choisissez le groupe auquel appartient l'utilisateur SNMP. Les groupes disponibles sont les suivants :

- **Auth&Encryption**, dans lequel les utilisateurs ont l'authentification et le chiffrement configurés
- **Authentication_Only**, dans lequel les utilisateurs n'ont que l'authentification configurée
- **No_Authentication**, dans lequel les utilisateurs n'ont ni l'authentification ni le chiffrement configurés

Remarque Vous ne pouvez pas modifier les noms de groupe.

Étape 4 Cliquez sur l'onglet **USM Model** (Modèle USM) pour utiliser les groupes de modèles de sécurité utilisateur (USM).

Étape 5 Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add SNMP USM Entry** (Ajouter une entrée USM SNMP) s'affiche.

Étape 6 Saisissez le nom du groupe.

Étape 7 Choisissez le niveau de sécurité dans la liste déroulante. Ce paramètre vous permet d'attribuer un groupe USM configuré comme niveau de sécurité aux utilisateurs SNMPv3.

Étape 8 Saisissez le nom d'un utilisateur configuré ou d'un nouvel utilisateur. Le nom d'utilisateur doit être unique pour le groupe de serveurs SNMP sélectionné.

Étape 9 Indiquez le type de mot de passe que vous souhaitez utiliser en cliquant sur l'un des deux boutons radio : **Encrypted** (Chiffré) ou **Clear Text** (Texte clair).

Étape 10 Indiquez le type d'authentification que vous souhaitez utiliser en cliquant sur l'un des quatre boutons radio : **SHA**, **SHA224**, **SHA256** ou **SHA384**.

Étape 11 Saisissez le mot de passe à utiliser pour l'authentification.

Étape 12 Indiquez le type de chiffrement que vous souhaitez utiliser en cliquant sur l'un de ces deux boutons radio : **3DES** ou **AES**.

Étape 13 Si vous avez choisi le chiffrement AES, choisissez le niveau de chiffrement AES à utiliser : **128**, **192** ou **256**.

Étape 14 Saisissez le mot de passe à utiliser pour le chiffrement. Le nombre maximal de caractères alphanumériques autorisé pour ce mot de passe est de 64.

Étape 15 Cliquez sur **OK** pour créer un groupe (s'il s'agit du premier utilisateur de ce groupe), affichez ce groupe dans la liste déroulante **Group Name** (Nom du groupe) et créez un utilisateur pour ce groupe.

La boîte de dialogue **Add SNMP User Entry** (Ajouter une entrée d'utilisateur SNMP) se ferme.

Étape 16 Cliquez sur **Apply** (Appliquer).

Les paramètres SNMP pour la version 3 sont configurés et les modifications sont enregistrées dans la configuration en cours d'exécution.

Configurer un groupe d'utilisateurs

Pour configurer une liste d'utilisateurs SNMP avec un groupe d'utilisateurs spécifiés, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP** .

Étape 2 Cliquez sur **Add (Ajouter)** > **SNMP User Group (Groupe d'utilisateurs SNMP)** sous l'onglet **SNMPv3 User/Group** (Utilisateur/Groupe SNMPv3) dans le volet **SNMPv3 Users** (Utilisateurs SNMPv3) pour ajouter un groupe d'utilisateurs configuré ou un nouveau groupe d'utilisateurs. Lorsque vous supprimez le dernier utilisateur d'un groupe, ASDM supprime le groupe.

La boîte de dialogue **Add SNMP User Group** (Ajouter un groupe d'utilisateurs SNMP) apparaît.

Étape 3 Saisissez le nom du groupe d'utilisateurs.

Étape 4 Cliquez sur le bouton radio **Existing User/User Group** (Utilisateur/Groupe d'utilisateurs existant) pour sélectionner un utilisateur ou un groupe d'utilisateurs existant.

Étape 5 Cliquez sur le bouton radio **Create new user** (Créer un nouvel utilisateur) pour créer un nouvel utilisateur.

Étape 6 Choisissez le groupe auquel appartient l'utilisateur SNMP. Les groupes disponibles sont les suivants :

- **Auth&Encryption**, dans lequel les utilisateurs ont l'authentification et le chiffrement configurés
- **Authentication_Only**, dans lequel les utilisateurs n'ont que l'authentification configurée
- **No_Authentication**, dans lequel les utilisateurs n'ont ni l'authentification ni le chiffrement configurés

Étape 7 Saisissez le nom d'un utilisateur configuré ou d'un nouvel utilisateur. Le nom d'utilisateur doit être unique pour le groupe de serveurs SNMP sélectionné.

Étape 8 Indiquez le type de mot de passe que vous souhaitez utiliser en cliquant sur l'un des deux boutons radio : **Encrypted** (Chiffré) ou **Clear Text** (Texte clair).

Étape 9 Indiquez le type d'authentification que vous souhaitez utiliser en cliquant sur l'un des quatre boutons radio : **SHA**, **SHA224**, **SHA256** ou **SHA384**.

Étape 10 Saisissez le mot de passe à utiliser pour l'authentification.

Étape 11 Confirmez le mot de passe à utiliser pour l'authentification.

Étape 12 Indiquez le type de chiffrement que vous souhaitez utiliser en cliquant sur l'un de ces deux boutons radio : **3DES** ou **AES**.

Étape 13 Saisissez le mot de passe à utiliser pour le chiffrement. Le nombre maximal de caractères alphanumériques autorisé pour ce mot de passe est de 64.

Étape 14 Confirmez le mot de passe à utiliser pour le chiffrement.

Étape 15 Cliquez sur **Add** (Ajouter) pour ajouter le nouvel utilisateur au groupe d'utilisateurs spécifié dans le volet **Members in Group** (Membres du groupe). Cliquez sur **Remove** (Supprimer) pour supprimer un utilisateur existant du volet **Members in Group** (Membres du groupe).

Étape 16 Cliquez sur **OK** pour créer un nouvel utilisateur pour le groupe d'utilisateurs spécifié.

La boîte de dialogue **Add SNMP User Group** (Ajouter un groupe d'utilisateurs SNMP) se ferme.

Étape 17 Cliquez sur **Apply** (Appliquer).

Les paramètres SNMP pour la version 3 sont configurés et les modifications sont enregistrées dans la configuration en cours d'exécution.

Supervision SNMP

Consultez les commandes suivantes pour superviser SNMP. Vous pouvez saisir ces commandes en sélectionnant **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**.

- **show running-config snmp-server** [**default**]

  Cette commande affiche tous les renseignements de configuration du serveur SNMP.

- **show running-config snmp-server group**

  Cette commande affiche les paramètres de configuration du groupe SNMP.

- **show running-config snmp-server host**

  Cette commande affiche les paramètres de configuration utilisés par SNMP pour contrôler les messages et les notifications envoyés aux hôtes distants.

- **show running-config snmp-server host-group**

  Cette commande affiche les configurations du groupe d'hôtes SNMP.

- **show running-config snmp-server user**

  Cette commande affiche les paramètres de configuration SNMP basés sur l'utilisateur.

- **show running-config snmp-server user-list**

  Cette commande affiche les configurations de la liste d'utilisateurs SNMP.

- **show snmp-server engineid**

  Cette commande affiche l'ID du moteur SNMP configuré.

- **show snmp-server group**

  Cette commande affiche les noms des groupes SNMP configurés. Si l'identifiant de communauté a déjà été configuré, deux groupes supplémentaires s'affichent par défaut dans la sortie. Ce comportement est normal.

- **show snmp-server statistics**

Cette commande affiche les caractéristiques configurées du serveur SNMP. Pour réinitialiser tous les compteurs SNMP à zéro, utilisez la commande **clear snmp-server statistics**.

- **show snmp-server user**

  Cette commande affiche les caractéristiques configurées des utilisateurs.

Historique de SNMP

Tableau 64 : Historique de SNMP

Nom de la caractéristique	Version	Description
SNMP versions 1 et 2c	7.0(1)	Fournit des renseignements sur la supervision du réseau ASA et les événements en transmettant les données entre le serveur SNMP et l'agent SNMP par l'identifiant de communauté en texte clair. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > SNMP.
SNMP version 3	8.2(1)	Fournit un chiffrement et une prise en charge 3DES ou AES pour SNMP version 3, la forme la plus sécurisée des modèles de sécurité pris en charge. Cette version vous permet de configurer les utilisateurs, les groupes et les hôtes, ainsi que les caractéristiques d'authentification à l'aide d'USM. En outre, cette version permet le contrôle d'accès à l'agent et aux objets MIB et comprend une prise en charge MIB supplémentaire. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > SNMP.
Chiffrement de mot de passe	8.3(1)	Prend en charge le chiffrement de mot de passe.
Alertes SNMP et MIB	v 8.4(1)	Prend en charge les mots clés supplémentaires suivants : **connection-limit-reached**, **cpu threshold rising**, **entity cpu-temperature**, **entity fan-failure**, **entity power-supply**, **ikev2 stop | start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**. Le tableau entPhysicalTable signale les entrées pour les capteurs, les ventilateurs, les alimentations et les composants connexes. Prend en charge les MIB supplémentaires suivantes : CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, DISMAN-EVENT-MIB, DISMAN-EXPRESSION-MIB, ENTITY-SENSOR-MIB, NAT-MIB. Prend en charge les interruptions supplémentaires suivantes : ceSensorExtThresholdNotification, clrResourceLimitReached, cpmCPURisingThreshold, mteTriggerFired, natPacketDiscard, warmStart. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > SNMP.

Nom de la caractéristique	Version	Description
Prise en charge de l'OID IF-MIB ifAlias	8.2(5)/8.4(2)	L'ASA prend désormais en charge l'OID ifAlias. Lorsque vous parcourez l'IF-MIB, l'OID ifAlias sera défini à la valeur qui a été définie pour la description de l'interface.
Module de services ASA (ASASM)	8.5(1)	L'ASASM prend en charge toutes les MIB et interruptions présentes dans 8.4(1), à l'exception des éléments suivants : MIB non prises en charge dans 8.5(1) : • CISCO-ENTITY-SENSOR-EXT-MIB (seuls les objets du groupe entPhySensorTable sont pris en charge). • ENTITY-SENSOR-MIB (seuls les objets du groupe entPhySensorTable sont pris en charge). • DISMAN-EXRPSION-MIB (seuls les objets des groupes expExpressionTable, expObjectTable et expValueTable sont pris en charge). Interruptions non prises en charge dans 8.5(1) : • ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB). Cette interruption est utilisée uniquement pour les défaillances d'alimentation, les défaillances de ventilateur et les événements de température élevée du processeur. • InterfacesBandwidthUtilization.
Interruptions SNMP	8.6(1)	Prend en charge les mots clés supplémentaires suivants pour les modèles ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X : **entity power-supply-presence**, **entity power-supply-failure**, **entity chassis-temperature**, **entity chassis-fan-failure, entity power-supply-temperature**. Nous avons modifié la commande suivante : **snmp-server enable traps**.
MIB liées au VPN	9.0(1)	Une version mise à jour de CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB a été implementée pour prendre en charge la fonctionnalité de chiffrement de nouvelle génération. Les MIB suivantes ont été activées pour l'ASASM : • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
MIB TrustSec de Cisco	9.0(1)	La prise en charge de la MIB suivante a été ajoutée : CISCO-TRUSTSEC-SXP-MIB.

Nom de la caractéristique	Version	Description
OID SNMP	9.1(1)	Cinq nouveaux OID de type prestataire physique SNMP ont été ajoutés pour prendre en charge les appareils ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X.
MIB NAT	9.1(2)	Ajout des OID cnatAddrBindNumberOfEntries et cnatAddrBindSessionCount pour prendre en charge les entrées xlate_count et max_xlate_count, qui sont équivalents à l'autorisation de l'interrogation à l'aide de la commande **show xlate count**.
Hôtes SNMP, groupes d'hôtes et listes d'utilisateurs	9.1(5)	Vous pouvez maintenant ajouter jusqu'à 4 000 hôtes. Le nombre de destinations d'interrogation actives prises en charge est de 128. Vous pouvez spécifier un objet réseau pour indiquer les hôtes individuels que vous souhaitez ajouter en tant que groupe d'hôtes. Vous pouvez associer plusieurs utilisateurs à un hôte. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > SNMP.
Taille des messages SNMP	9.2(1)	La limite de taille des messages que SNMP envoie a été augmentée à 1 472 octets.
OID et MIB SNMP	9.2(1)	L'ASA prend désormais en charge l'OID cpmCPUTotal5minRev. L'ASA virtuel a été ajouté en tant que nouveau produit aux OID sysObjectID et entPhysicalVendorType de SNMP. Les fichiers CISCO-PRODUCTS-MIB et CISCO-ENTITY-VENDORTYPE-OID-MIB ont été mis à jour pour prendre en charge la nouvelle plateforme ASA virtuel. Une nouvelle MIB SNMP pour superviser l'utilisation des licences partagées des VPN a été ajoutée.
OID et MIB SNMP	9.3(1)	La prise en charge de CISCO-REMOTE-ACCESS-MONITOR-MIB (OID 1.3.6.1.4.1.9.9.392) a été ajoutée pour l'ASASM.

Nom de la caractéristique	Version	Description
MIB et alertes SNMP	9.3(2)	Les fichiers CISCO-PRODUCTS-MIB et CISCO-ENTITY-VENDORTYPE-OID-MIB ont été mis à jour pour prendre en charge l'ASA 5506-X. L'ASA 5506-X a été ajouté en tant que nouveau produit aux tableaux d'OID sysObjectID et entPhysicalVendorType de SNMP. L'ASA prend désormais en charge CISCO-CONFIG-MAN-MIB, qui vous permet de faire les opérations suivantes : • Savoir quelles commandes ont été saisies pour une configuration en particulier. • Avertir le NMS lorsqu'une modification s'est produite dans la configuration d'exécution. • Suivez les horodatages associés à la dernière fois que la configuration d'exécution a été modifiée ou enregistrée. • Suivez les autres modifications apportées aux commandes, comme les détails du terminal et les sources de commandes. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > SNMP > Configure Traps (Configurer les interruptions) > SNMP Trap Configuration (Configuration des alertes SNMP).
MIB et alertes SNMP	9.4(1)	Les ASA 5506W-X, ASA 5506H-X, ASA 5508-X et ASA 5516-X ont été ajoutés en tant que nouveaux produits aux tableaux d'OID sysObjectID et entPhysicalVendorType de SNMP.
Hôtes d'interruption de serveur SNMP illimités par contexte	9.4(1)	L'ASA prend en charge un nombre illimité d'hôtes d'interruption de serveur SNMP par contexte. La sortie de la commande **show snmp-server host** affiche uniquement les hôtes actifs qui interrogent l'ASA, ainsi que les hôtes configurés de manière statique. Nous n'avons pas modifié d'écrans ASDM.
Ajout de la prise en charge pour ISA 3000	9.4(1.225)	La gamme de produits ISA 3000 est désormais prise en charge pour SNMP. Nous avons ajouté de nouveaux OID pour cette plateforme. La commande **snmp-server enable traps entity** a été modifiée pour inclure une nouvelle variable *l1-bypass-status*. Cela active le changement d'état du contournement matériel. Nous n'avons pas modifié d'écrans ASDM.
Prise en charge de cempMemPoolTable dans CISCO-ENHANCED-MEMPOOL-MIB	9.6(1)	Le tableau cempMemPoolTable de CISCO-ENHANCED-MEMPOOL-MIB est maintenant pris en charge. Il s'agit d'un tableau des entrées de surveillance de la réserve de mémoire pour toutes les entités physiques d'un système géré. **Remarque** CISCO-ENHANCED-MEMPOOL-MIB utilise des compteurs de 64 bits et prend en charge les rapports de mémoire sur les plateformes avec plus de 4 Go de RAM.

Nom de la caractéristique	Version	Description
Prise en charge des MIB en mode d'horloge E2E transparent pour le protocole PTP (Precision Time Protocol)	9.7(1)	Les MIB correspondant au mode d'horloge E2E transparent sont maintenant prises en charge. **Remarque** Seules les opérations SNMP get, bulkget, getnext et walk sont prises en charge.
SNMP sur IPv6	9.9(2)	L'ASA prend désormais en charge SNMP sur IPv6, y compris la communication avec des serveurs SNMP sur IPv6, permettant l'exécution de requêtes et d'interruptions sur IPv6 et prenant en charge les adresses IPv6 pour les MIB existantes. Nous avons ajouté les nouveaux objets MIB IPv6 SNMP suivants, comme décrit dans la RFC 8096. • ipv6InterfaceTable (OID : 1.3.6.1.2.1.4.30) : contient des renseignements spécifiques à IPv6 par interface. • ipAddressPrefixTable (OID :1.3.6.1.2.1.4.32) : comprend tous les préfixes appris par cette entité. • ipAddressTable (OID : 1.3.6.1.2.1.4.34) : contient des renseignements d'adressage pertinents pour les interfaces de l'entité. • ipNetToPhysicalTable (OID : 1.3.6.1.2.1.4.35) : contient le mappage des adresses IP aux adresses physiques. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP**
Prise en charge de l'activation et de la désactivation des résultats de la mémoire libre et des statistiques de mémoire utilisée lors des opérations de marche SNMP	9.10(1)	Pour éviter la surutilisation des ressources du processeur, vous pouvez activer et désactiver la requête de mémoire libre et les statistiques de mémoire utilisée collectées par les opérations de marche de SNMP. Nous n'avons pas modifié d'écrans ASDM.
Prise en charge de l'activation et de la désactivation des résultats de la mémoire libre et des statistiques de mémoire utilisée lors des opérations de marche SNMP	9.12(1)	Pour éviter la surutilisation des ressources du processeur, vous pouvez activer et désactiver la requête de mémoire libre et les statistiques de mémoire utilisée collectées par les opérations de marche de SNMP. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP**
Authentification SNMPv3	9.14(1)	Vous pouvez maintenant utiliser le code HMAC SHA-256 pour l'authentification de l'utilisateur. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP**
Pour les paires de basculements en version 9.14(1) ou toute version ultérieure, l'ASA ne partage plus les données du moteur client SNMP avec son homologue.	9.14(1)	L'ASA ne partage plus les données du moteur client SNMP avec son homologue.

Nom de la caractéristique	Version	Description
Interrogation SNMP sur le VPN de site à site	9.14(2)	Pour une interrogation SNMP sécurisée sur un VPN de site à site, incluez l'adresse IP de l'interface externe dans la liste d'accès de la carte cryptographique dans le cadre de la configuration du VPN.
La prise en charge des OID CISCO-MEMORY-POOL-MIB est rendue obsolète	9.15(1)	Les OID CISCO-MEMORY-POOL-MIB (ciscoMemoryPoolUsed, ciscoMemoryPoolFree) sont obsolètes pour les systèmes qui utilisent des compteurs de 64 bits. Le tableau cempMemPoolTable de CISCO-ENHANCED-MEMPOOL-MIB fournit des entrées de supervision de la réserve de mémoire pour les systèmes qui utilisent des compteurs de 64 bits.
Authentification SNMPv3	9.16(1)	Vous pouvez maintenant utiliser SHA-224 et SHA-384 pour l'authentification de l'utilisateur. Vous ne pouvez plus utiliser MD5 pour l'authentification de l'utilisateur. Vous ne pouvez plus utiliser DES pour le chiffrement. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **SNMP**
Prise en charge de l'interface de boucle avec retour pour SNMP	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour SNMP. Commandes nouvelles/modifiées : **interface loopback**, **snmp-server host** Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add Loopback Interface (ajouter une interface de bouclage)**. La prise en charge d'ASDM a été ajoutée dans la version 7.19.



CHAPITRE 50

Données de télémétrie et du Cisco Success Network

Ce chapitre décrit le Cisco Success Network et comment l'activer sur l'ASA. Il répertorie également les points de données télémétriques qui sont envoyés au nuage Security Service Engine (SSE).

- À propos de Cisco Success Network , à la page 1321
- Activer ou désactiver Cisco Success Network , à la page 1322
- Afficher les données de télémétrie d'ASA , à la page 1323
- Cisco Success Network – Données de télémétrie, à la page 1323

À propos de Cisco Success Network

Cisco Success Network est un service en nuage activé par l'utilisateur qui établit une connexion sécurisée avec le nuage Security Service Exchange (SSE) afin de diffuser en continu les renseignements et les statistiques d'utilisation de l'ASA. La télémétrie en continu fournit un mécanisme permettant de transmettre l'utilisation de l'ASA et d'autres détails dans un format structuré (JSON) à des stations de gestion à distance, ce qui présente les avantages suivants :

- Pour vous informer des services de soutien technique supplémentaires et de la supervision offerte pour votre produit.
- Pour aider Cisco à améliorer ses produits.

Par défaut, Cisco Success Network est activé sur les plateformes Firepower 4100/9300 qui hébergent les périphériques ASA (au niveau de la lame). Cependant, pour que les données de télémétrie soient transmises, vous devez activer la configuration sur FXOS au niveau du châssis (consultez le Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS) ou activez le Cisco Success Network sur le gestionnaire de châssis (consultez le Guide de configuration du Firepower Chassis Manager de Cisco Firepower Cisco Firepower 4100/9300 FXOS). L'ASA vous permet de désactiver le service de télémétrie à tout moment.

Les données de télémétrie collectées sur vos périphériques ASA comprennent l'utilisation du processeur, de la mémoire, du disque, de la bande passante et des licences, la liste des fonctionnalités configurées, les renseignements sur la grappe et le basculement, etc. Veuillez vous référer à Cisco Success Network – Données de télémétrie, à la page 1323.

Plateformes prises en charge et configurations requises

- Pris en charge sur les plateformes FP9300/4100 avec l'ASA version 9.13.1 ou supérieure.
- Nécessite FXOS version 2.7.1 ou ultérieure pour la connexion au nuage.
- Le connecteur SSE sur FXOS doit être connecté au nuage SSE. Cette connexion est établie par l'activation et l'enregistrement de la licence Smart avec le système dorsal de licence Smart. Le connecteur SSE sur FXOS est automatiquement enregistré dans le nuage SSE lors de l'enregistrement de la licence Smart.
- La configuration de Cisco Success Network doit être activée sur le gestionnaire de châssis.
- La configuration de télémétrie doit être activée sur l'ASA.

Comment les données de télémétrie ASA atteignent le nuage SSE

Cisco Success Network est pris en charge sur les plateformes Firepower 4100/9300 dans l'ASA 9.13(1) par défaut. Le gestionnaire de service FXOS envoie quotidiennement des requêtes de télémétrie à l'application ASA en cours d'exécution sur la plateforme. Le moteur ASA, en fonction de l'état de configuration et de connectivité, envoie les données de télémétrie en mode autonome ou en mode grappe à FXOS. En d'autres termes, si la prise en charge de la télémétrie est activée dans l'ASA et que le connecteur SSE est connecté, le fil de télémétrie extrait les renseignements nécessaires de diverses sources telles que les API de système, de plateforme ou d'appareil, les API de licence, les API de CPU, les API de mémoire, les API de disque, les API de la fonction Smart Call Home, etc. Cependant, si la prise en charge de la télémétrie est désactivée dans l'ASA ou que le connecteur SSE est déconnecté, l'ASA envoie une réponse à FXOS (appAgent) indiquant l'état de la configuration de la télémétrie et n'envoie aucune donnée de télémétrie.

FXOS n'a qu'une seule instance de connecteur SSE en cours d'exécution. Lorsqu'il est enregistré auprès du nuage SSE, il est considéré comme un seul périphérique et l'infrastructure SSE attribue à FXOS un ID de périphérique. Tout rapport de télémétrie envoyé par le biais du connecteur SSE est classé sous le même ID de périphérique. Par conséquent, FXOS regroupe les rapports de télémétrie de chaque ASA en un seul rapport. D'autres contenus, tels que les renseignements sur le compte de licence Smart, sont ajoutés au rapport. FXOS envoie ensuite le rapport final au nuage SSE. Les données de télémétrie sont enregistrées dans l'échange de données SSE (DX) et sont disponibles pour l'équipe informatique de Cisco.

Activer ou désactiver Cisco Success Network

Avant de commencer

- Activez et enregistrez la licence Smart sur FXOS.
- Activez la prise en charge de la télémétrie sur FXOS au niveau du châssis (consultez le Guide de configuration de l'interface de ligne de commande de Cisco Firepower 4100/9300 FXOS) ou activez le Cisco Success Network sur le gestionnaire de châssis (consultez le Guide de configuration du Firepower Chassis Manager de Cisco Firepower 4100/9300 FXOS).

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Telemetry (Télémétrie)**.

La case **Enable Cisco Success Network** (Activer Cisco Success Network) est cochée par défaut.

Étape 2 Assurez-vous que Cisco Success Network est activé en cochant la case **Enable Cisco Success Network** (Activer Cisco Success Network).

Étape 3 Pour désactiver Cisco Success Network, décochez la case **Enable Cisco Success Network** (Activer Cisco Success Network).

Étape 4 Cliquez sur **Apply** (Appliquer).

Prochaine étape

- Vous pouvez afficher la configuration et le journal des activités de télémétrie ou les données de télémétrie. Voir la section Afficher les données de télémétrie d'ASA , à la page 1323.
- Pour afficher un exemple de données de télémétrie et de champs de données, consultez Cisco Success Network – Données de télémétrie, à la page 1323

Afficher les données de télémétrie d'ASA

Avant de commencer

- Activez le service de télémétrie sur l'ASA. Voir la section Activer ou désactiver Cisco Success Network , à la page 1322.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Telemetry (Télémétrie)**.

Étape 2 Sous **Telemetry** (Télémétrie), cliquez sur l'option appropriée :

- **History** (Historique) : pour afficher les 100 derniers événements liés à la configuration et aux activités de télémétrie.
- **Sample** (Échantillon) : pour afficher les données de télémétrie générées instantanément au format JSON.
- **Last-report** (Dernier rapport) : pour afficher les dernières données de télémétrie envoyées à FXOS au format JSON.

Étape 3 Cliquez sur **Refresh** (Actualiser) pour afficher le rapport.

Cisco Success Network – Données de télémétrie

Cisco Success Network est pris en charge sur les plateformes Firepower 4100/9300 par défaut. Le gestionnaire de service FXOS envoie quotidiennement des requêtes de télémétrie au moteur ASA en cours d'exécution sur la plateforme. Le moteur ASA, en cas de réception de la demande, en fonction de l'état de la connectivité,

envoie les données de télémétrie en mode autonome ou en mode grappe à FXOS. Les tableaux suivants fournissent des renseignements sur les points de données de télémétrie, leur description et des exemples de valeurs.

Tableau 65 : Renseignements sur le périphérique

Point de données	Description	Exemple de valeur
Modèle du périphérique	le modèle d'appareil (Device model)	Appareils de sécurité adaptatifs de Cisco
Serial Number (numéro de série)	Numéro de série de l'appareil	FCH183771EZ
Heure système	Disponibilité du système	11658000
Observations	Matériel	FPR9K-SM-24
Mode de déploiement	Type de déploiement	Natif
Mode de contexte de sécurité	Unique/Multiple	Unique

Tableau 66 : Renseignements sur les versions

Point de données	Description	Exemple de valeur
Variable globale de version	Version d'ASA	9.13.1.5
Version de gestionnaire d'appareil	Version de gestionnaire d'appareil	7.10.1

Tableau 67 : Renseignements de licence

Point de données	Description	Exemple de valeur
Variable globale de la licence Smart	Licences activées	regid.2015-01.com.cisco.ASA - SSP-STRONG-ENCRYPTION, 1.0_555507e9-85f8-4e41-96de-860b59f10bbe

Tableau 68 : Renseignements sur la plateforme

Point de données	Description	Exemple de valeur
UC	Utilisation du CPU au cours des 5 dernières minutes	fiveSecondsPercentage : 0.2000000, oneMinutePercentage : 0, fiveMinutesPercentage : 0

Point de données	Description	Exemple de valeur
Mémoire	Utilisation de la mémoire	freeMemoryInBytes : 225854966384, usedMemoryInBytes : 17798281616, totalMemoryInBytes : 243653248000
Disque	Utilisation du disque	freeGB : 21.237285, usedGB : 0.238805, totalGB : 21.476090
Bande passante	Utilisation de la bande passante	receivedPktsPerSec : 3, receivedBytesPerSec : 212, transmittedPktsPerSec : 3, transmittedBytesPerSec : 399

Tableau 69 : Renseignements sur les fonctionnalités

Point de données	Description	Exemple de valeur
Liste des fonctionnalités	Liste des fonctionnalités activées	nom : grappe état : activé

Tableau 70 : Renseignements sur la grappe

Point de données	Description	Exemple de valeur
Renseignements sur la grappe	Renseignements sur la grappe	clusterGroupName : ssp-cluster interfaceMode : spanned unitName : unit-3-3 unitState : SLAVE otherMembers : items : memberName : unit-2-1 memberState : MASTER memberSerialNum : FCH183771BA

Tableau 71 : Renseignements sur le basculement

Point de données	Description	Exemple de valeur
Basculement	Renseignements sur le basculement	myRole : Primary, peerRole : Secondary, myState : active, peerState : standby, peerSerialNum : FCH183770EZ

Tableau 72 : Renseignements de connexion

Point de données	Description	Exemple de valeur
Ouvrir une session	Historique de connexion	loginTimes : 2 fois dans les 2 derniers jours, lastSuccessfulLogin : 12:25:36 (HAP) 11 mars 2019

Exemple de données de télémétrie ASA

Voici un exemple des données de télémétrie envoyées par l'ASA au format JSON. Lorsque le gestionnaire de service reçoit cette entrée, il regroupe les données de tous les ASA et ajoute les en-têtes et les champs nécessaires avant de les envoyer au connecteur SSE. Les en-têtes/champs comprennent « version », « metadata », « payload » avec « recordedAt », « recordType », « recordVersion » et des données de télémétrie ASA, « smartLicenseProductInstanceIdentifier », « smartLicenseVirtualAccountName », etc.


```
{
  "version": "1.0",
  "metadata": {
    "topic": "ASA.telemetry",
    "contentType": "application/json"
  },
  "payload": {
    "recordType": "CST_ASA",
    "recordVersion": "1.0",
    "recordedAt": 1557363423705,
    "SSP": {
      "SSPdeviceInfo": {
        "deviceModel": "Cisco Firepower FP9300 Security Appliance",
        "serialNumber": "JMX2235L01J",
        "smartLicenseProductInstanceIdentifier": "f85a5bb0-xxxx-xxxx-xxxx-xxxxxxxxx",
        "smartLicenseVirtualAccountName": "SSP-general",
        "systemUptime": 198599,
        "udiProductIdentifier": "FPR-C9300-AC"
      },
      "versions": {
        "items": [
          {
            "type": "package_version",
            "version": "92.7(1.342g)"
          }
        ]
      }
    },
```

```
    "asaDevices": {
      "items": [
        {
    "deviceInfo": {
        "deviceModel": "Cisco Adaptive Security Appliance",
        "serialNumber": "AANNNXXX",
        "systemUptime": 285,
        "udiProductIdentifier": "FPR9K-SM-36",
        "deploymentType": "Native",
        "securityContextMode": "Single"
    },
    "versions": {
        "items": [
            {
                "type": "asa_version",
                "version": "201.4(1)82"
            },
            {
                "type": "device_mgr_version",
                "version": "7.12(1)44"
            }
        ]
    },
    "licenseActivated": {
        "items": [
            {
                "type": "Strong encryption",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-STRONG-ENCRYPTION,1.0_xxxxxxx-xxxx-xxxx-96de-860b59f10bbe",

                "count": 1
            },
            {
                "type": "Carrier",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-MOBILE-SP,1.0_xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
                "count": 1
            }
        ]
    },
    "CPUUsage": {
        "fiveSecondsPercentage": 0,
        "oneMinutePercentage": 0,
        "fiveMinutesPercentage": 0
    },
    "memoryUsage": {
        "freeMemoryInBytes": 99545662064,
        "usedMemoryInBytes": 20545378704,
        "totalMemoryInBytes": 120091040768
    },
    "diskUsage": {
        "freeGB": 21.237027,
        "usedGB": 0.239063,
        "totalGB": 21.476090
    },
    "bandwidthUsage": {
        "receivedPktsPerSec": 3,
        "receivedBytesPerSec": 268,
        "transmittedPktsPerSec": 4,
        "transmittedBytesPerSec": 461
    },
    "featureStatus": {
        "items": [
            {
```

```
        "name": "call-home",
        "status": "enabled"
    },
    {
        "name": "cluster",
        "status": "enabled"
    },
    {
        "name": "firewall_user_authentication",
        "status": "enabled"
    },
    {
        "name": "inspection-dns",
        "status": "enabled"
    },
    {
        "name": "inspection-esmtp",
        "status": "enabled"
    },
    {
        "name": "inspection-ftp",
        "status": "enabled"
    },
    {
        "name": "inspection-netbios",
        "status": "enabled"
    },
    {
        "name": "inspection-rsh",
        "status": "enabled"
    },
    {
        "name": "inspection-sip",
        "status": "enabled"
    },
    {
        "name": "inspection-sqlnet",
        "status": "enabled"
    },
    {
        "name": "inspection-sunrpc",
        "status": "enabled"
    },
    {
        "name": "inspection-tftp",
        "status": "enabled"
    },
    {
        "name": "inspection-xdmcp",
        "status": "enabled"
    },
    {
        "name": "logging-console",
        "status": "informational"
    },
    {
        "name": "management-mode",
        "status": "normal"
    },
    {
        "name": "sctp-engine",
        "status": "enabled"
    },
    {
```

```
                    "name": "threat_detection_basic_threat",
                    "status": "enabled"
                },
                {
                    "name": "threat_detection_stat_access_list",
                    "status": "enabled"
                },
                {
                    "name": "webvpn-activex-relay",
                    "status": "enabled"
                },
                {
                    "name": "webvpn-dtls",
                    "status": "enabled"
                }
            ]
        },
        "clusterInfo": {
            "clusterGroupName": "ssp-cluster",
            "interfaceMode": "spanned",
            "unitName": "unit-3-3",
            "unitState": "SLAVE",
            "otherMembers": {
                "items": [
                    {
                        "memberName": "unit-2-1",
                        "memberState": "MASTER",
                        "memberSerialNum": "FCH183771BA"
                    },
                    {
                        "memberName": "unit-2-3",
                        "memberState": "SLAVE",
                        "memberSerialNum": "FLM1949C6JR"
                    },
                    {
                        "memberName": "unit-2-2",
                        "memberState": "SLAVE",
                        "memberSerialNum": "xxxxxxxx"
                    },
                    {
                        "memberName": "unit-3-2",
                        "memberState": "SLAVE",
                        "memberSerialNum": "xxxxxxxx"
                    },
                    {
                        "memberName": "unit-3-1",
                        "memberState": "SLAVE",
                        "memberSerialNum": "xxxxxxxx"
                    }
                ]
            }
        },
        "loginHistory": {
            "loginTimes": "1 times in last 1 days",
            "lastSuccessfulLogin": "12:25:36 PDT Mar 11 2019"
        }
    }
```



CHAPITRE 51

Alarmes pour Cisco ISA 3000

Ce chapitre donne un aperçu du système d'alarme dans l'ISA 3000 et décrit également comment configurer et superviser les alarmes.

- À propos des alarmes, à la page 1331
- Valeurs par défaut pour les alarmes, à la page 1333
- Configurer les alarmes, à la page 1333
- Surveillance des alarmes, à la page 1335
- Historique des alarmes, à la page 1336

À propos des alarmes

Vous pouvez configurer l'ISA 3000 pour qu'il émette des alarmes dans diverses conditions. Si les conditions ne correspondent pas aux paramètres configurés, le système déclenche une alarme, qui est signalée par des DEL, des messages du journal système, des déroutements SNMP et par des périphériques externes connectés à l'interface de sortie d'alarme. Par défaut, les alarmes déclenchées n'émettent que des messages syslog.

Vous pouvez configurer le système d'alarme pour surveiller les éléments suivants :

- Bloc d'alimentation
- Capteurs de température principal et secondaire.
- Interfaces d'entrée d'alarme.

L'ISA 3000 est doté de capteurs internes ainsi que de deux interfaces d'entrée d'alarme et d'une interface de sortie d'alarme. Vous pouvez connecter des capteurs externes, comme des capteurs de porte, aux entrées d'alarme. Vous pouvez connecter des périphériques d'alarme externes, comme des avertisseurs sonores ou des voyants, à l'interface de sortie d'alarme.

L'interface de sortie d'alarme est un mécanisme de relais. Selon les conditions d'alarme, le relais est soit activé ou désactivé. Lorsqu'elle est sous tension, tout périphérique connecté à l'interface est activé. Un relais hors tension entraîne l'état inactif de tous les périphériques connectés. Le relais reste activé tant que des alarmes sont déclenchées.

Pour en savoir plus sur la connexion des capteurs externes et le relais d'alarme, consultez la section Alarmes pour le chapitre Cisco ISA 3000 dans le Guide de configuration de l'interface CLI pour les opérations générales Cisco ASA. Consultez le Guide d'installation du matériel pour l'appareil de sécurité industriel Cisco ISA 3000.

Interfaces d'entrée d'alarme.

Vous pouvez connecter les interfaces d'entrée (ou contacts) d'entrée d'alarme à des capteurs externes, par exemple celui qui détecte si une porte est ouverte.

Chaque interface d'entrée d'alarme a un voyant DEL correspondant. Ces voyants DEL transmettent l'état d'alarme de chaque entrée d'alarme. Vous pouvez configurer le déclencheur et la gravité de chaque entrée d'alarme. En plus du voyant DEL, vous pouvez configurer le contact pour déclencher le relais de sortie (pour activer une alarme externe), pour envoyer des messages syslog et pour envoyer des déroutements SNMP.

Le tableau suivant explique les états des voyants DEL en réponse aux conditions d'alarme pour les entrées d'alarme. Il explique également le comportement du relais de sortie, des messages du journal système et des interruptions SNMP, si vous activez ces réponses pour l'entrée d'alarme.

État de l'alarme	DEL	Relais de sortie	Syslog	Interruptions SNMP
Alarme non configurée	Désactivé	—	—	—
Aucune alarme déclenchée	Vert fixe	—	—	—
Alarme activée	Alarme mineure : rouge fixe Alarme majeure : rouge clignotant	Relais sous tension	Journal système généré	Déroutement SNMP envoyé.
Fin d'alarme	Vert fixe	Relais désactivé	Journal système généré	—

Interface de sortie d'alarme

Vous pouvez connecter une alarme externe, comme un avertisseur ou un voyant, à l'interface de sortie d'alarme.

L'interface de sortie d'alarme fonctionne comme un relais et est également dotée d'un voyant DEL correspondant, qui transmet l'état d'alarme d'un capteur externe connecté à l'interface d'entrée et des capteurs internes tels que la double alimentation et les capteurs de température. Vous configurez les alarmes qui doivent activer le relais de sortie, le cas échéant.

Le tableau suivant explique les états des DEL et du relais de sortie en réponse à des conditions d'alarme. Elle explique également le comportement des messages syslog et des alertes SNMP si vous activez ces réponses à l'alarme.

État de l'alarme	DEL	Relais de sortie	Syslog	Interruptions SNMP
Alarme non configurée	Désactivé	—	—	—
Aucune alarme déclenchée	Vert fixe	—	—	—
Alarme activée	Rouge fixe	Relais sous tension	Journal système généré	Déroutement SNMP envoyé.

État de l'alarme	DEL	Relais de sortie	Syslog	Interruptions SNMP
Fin d'alarme	Vert fixe	Relais désactivé	Journal système généré	—

Valeurs par défaut pour les alarmes

Le tableau suivant précise les valeurs par défaut pour les interfaces d'entrée d'alarme (contacts), l'alimentation redondante et la température.

	Alerte	initiales	Gravité	Interruptions SNMP	Relais de sortie	Messages de journalisation du système (syslog)
Contact d'alarme 1	Activé	État fermé	Mineur	Désactivé	Désactivé	Activé
Contact d'alarme 2	Activé	État fermé	Mineur	Désactivé	Désactivé	Activé
Alimentation redondante (si activée)	Activé	—	—	Désactivé	Désactivé	Activé
Température	Activé pour l'alarme de température principale (valeurs par défaut de 92 °C et de -40 °C pour les seuils respectivement) Désactivé pour l'alarme secondaire.	—	—	Activé pour l'alarme de température principale	Activé pour l'alarme de température principale	Activé pour l'alarme de température principale

Configurer les alarmes

Pour configurer des alarmes pour ISA 3000, procédez comme suit.

Procédure

Étape 1 Configurez les alarmes, la supervision et la journalisation dans le volet de contact des alarmes requises.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Alarm Port (Port d'alarme)** > **Alarm Contact (Contact d'alarme)**.
b) Cliquez sur le bouton radio **major** (majeure) ou **minor** (mineure) pour spécifier la gravité. Cliquez sur **none** (aucune) pour désactiver l'alarme de gravité.
c) Cliquez sur le bouton radio **open** (ouvert) ou **closed** (fermé) pour spécifier le déclencheur.

   La valeur par défaut est closed (fermé). Si vous spécifiez open (ouvert), une alarme se déclenchera lorsqu'un contact normalement fermé est ouvert ou lorsque le courant cesse de circuler. Si vous spécifiez closed (fermé), une alarme se déclenchera lorsque le contact normalement ouvert est fermé ou lorsque le courant commence à circuler.

   Par exemple, si un capteur de porte est connecté à une entrée d'alarme, son état normalement ouvert n'a pas de courant électrique circulant à travers les contacts. Si la porte est ouverte, le courant électrique circule à travers les contacts, activant l'alarme.

d) (Facultatif) Entrez la description dans le champ **Description**. La description peut comporter jusqu'à 80 caractères alphanumérique et sera incluse dans les messages du journal système.
e) Cochez la case **Enable relay** (Activer le relais).
f) Cochez la case **Enable system logger** (Activer la journalisation du système) pour activer les journaux système.
g) Cochez la case **Enable notification sent to server** (Activer la notification envoyée au serveur) pour activer les alertes SNMP.
h) Cliquez sur **Apply** (Appliquer).

Étape 2 Configurez l'alarme, la supervision et la journalisation pour l'alimentation redondante.

L'alimentation redondante doit être activée pour que les alarmes d'alimentation fonctionnent.

Pour activer l'alimentation redondante, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Power Supply (Alimentation)**. Cochez la case **Enable Redundant Power Supply** (Activer l'alimentation redondante), puis cliquez sur **Apply** (Appliquer).

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Alarm Port (Port d'alarme)**.
b) Cliquez sur l'onglet **Redundant Power Supply** (Alimentation redondante).
c) Cochez la case **Enable notification sent to server** (Activer la notification envoyée au serveur) pour activer les alertes SNMP.
d) Cochez la case **Enable relay** (Activer le relais).
e) Cochez la case **Enable system logger** (Activer la journalisation du système) pour activer les journaux système.
f) Cliquez sur **Apply** (Appliquer).

Étape 3 Configurez les alarmes, la supervision et la journalisation, pour la température.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Alarm Port (Port d'alarme)**.
b) Cliquez sur l'onglet **Temperature** (Température).
c) Cochez la case **Enable notification sent to server** (Activer la notification envoyée au serveur) pour activer les alertes SNMP.
d) Cochez la case **Enable relay** (Activer le relais).
e) Cochez la case **Enable system logger** (Activer la journalisation du système) pour activer les journaux système.
f) Saisissez les seuils supérieur et inférieur dans les champs **High Threshold** (Seuil supérieur) et **Low Threshold** (Seuil inférieur) dans le volet d'alarmes requises.

Pour l'alarme de température principale, les valeurs valides sont comprises entre -40 °C et 92 °C. Pour l'alarme de température secondaire, les valeurs valides sont comprises entre -35 °C et 85 °C. Si un seuil de température élevée est configuré pour l'alarme secondaire, seule l'alarme secondaire sera activée. L'alarme principale ne peut pas être désactivée. Lorsque les valeurs de seuil ne sont pas spécifiées pour l'alarme principale, elle revient aux valeurs par défaut de 92 °C et de -40 °C pour les seuils supérieur et inférieur, respectivement.

g) Cliquez sur **Apply** (Appliquer).

Surveillance des alarmes

Consultez les volets suivants pour superviser les alarmes

Procédure

- Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Alarm (Alarme)** > **Alarm Settings (Paramètres d'alarme)**.

  Ce volet affiche tous les paramètres d'alarme globaux.

- Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Alarm (Alarme)** > **Alarm Contact (Contact d'alarme)**.

  Ce volet affiche tous les paramètres d'alarme externe.

- Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Alarm (Alarme)** > **Facility Alarm Status (État d'alarme de l'installation)**.

  Ce volet affiche toutes les alarmes en fonction de la gravité spécifiée et affiche les renseignements suivants :

Colonne	Description
Source	Périphérique à partir duquel l'alarme a été déclenchée. Il s'agit généralement du nom d'hôte configuré sur le périphérique.
Gravité	Majeure ou mineure
Description	Type d'alarme déclenchée. Par exemple, la température, le contact externe, l'alimentation redondante, etc.
Relais	Sous tension ou hors tension
Durée	Horodatage de l'alarme déclenchée

Historique des alarmes

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge des ports d'alarme pour l'ISA 3000	9.7(1)	L'ISA 3000 prend désormais en charge deux broches d'entrée d'alarme et une broche de sortie d'alarme, avec des voyants DEL pour indiquer l'état des alarmes. Des capteurs externes peuvent être connectés aux entrées d'alarme. Un relais matériel externe peut être connecté à la broche de sortie d'alarme. Vous pouvez configurer les descriptions des alarmes externes. Vous pouvez également indiquer la gravité et le déclencheur pour les alarmes externes et internes. Toutes les alarmes peuvent être configurées pour le relais, la supervision et la journalisation. Nous avons introduit les commandes suivantes : **alarm contact description, alarm contact severity, alarm contact trigger, alarm facility input-alarm, alarm facility power-supply rps, alarm facility temperature, alarm facility temperature high, alarm facility temperature low, clear configure alarm, clear facility-alarm output, show alarm settings, show environment alarm-contact**. Nous avons introduit les écrans suivants : **Configuration** > **Device Management (Gestion des périphériques)** > **Alarm Port (Port d'alarme)** > **Alarm Contact (Contact d'alarme)** **Configuration** > **Device Management (Gestion des périphériques)** > **Alarm Port (Port d'alarme)** > **Redundant Power Supply (Bloc d'alimentation redondant)** **Configuration** > **Device Management (Gestion des périphériques)** > **Alarm Port (Port d'alarme)** > **Temperature (Température)** **Monitoring (Supervision)** > **Properties (Propriétés)** > **Alarm (Alarme)** > **Alarm Settings (Paramètres d'alarme)** **Monitoring (Supervision)** > **Properties (Propriétés)** > **Alarm (Alarme)** > **Alarm Contact (Contact d'alarme)** **Monitoring (Supervision)** > **Properties (Propriétés)** > **Alarm (Alarme)** > **Facility Alarm Status (État d'alarme de l'installation)**



CHAPITRE 52

Rapports anonymes et Smart Call Home

Ce chapitre décrit comment configurer les services de création de rapports anonymes et les services Smart Call Home.

- À propos des rapports anonymes, à la page 1337
- À propos de Smart Call Home, à la page 1338
- Lignes directrices relatives aux rapports anonymes et à Smart Call Home, à la page 1339
- Configurer les rapports anonymes et Smart Call Home, à la page 1340
- Supervision des rapports anonymes et de Smart Call Home, à la page 1345
- Historique des rapports anonymes et de Smart Call Home, à la page 1346

À propos des rapports anonymes

Vous pouvez contribuer à l'amélioration de la plateforme ASA en activant les rapports anonymes, qui permettent à Cisco de recevoir en toute sécurité un minimum de renseignements sur les erreurs et l'intégrité de l'appareil. Si vous activez la fonctionnalité, votre identité de client restera anonyme et aucune information d'identification ne sera envoyée.

L'activation de la création de rapports anonymes crée un point de confiance et installe un certificat. Un certificat CA est requis pour que votre ASA valide le certificat de serveur présent sur le serveur Web Smart Call Home et pour former la session HTTPS afin que votre ASA puisse envoyer des messages en toute sécurité. Cisco importe un certificat prédéfini dans le logiciel. Si vous décidez d'activer les rapports anonymes, un certificat est installé sur l'ASA avec un nom de point de confiance codé en dur : _SmartCallHome_ServerCA. Lorsque vous activez la création de rapports anonymes, ce point de confiance est créé, le certificat approprié est installé et vous recevez un message au sujet de cette action. Le certificat apparaît ensuite dans votre configuration.

Si le certificat approprié existe déjà dans votre configuration lorsque vous activez les rapports anonymes, aucun point de confiance n'est créé et aucun certificat n'est installé.

Remarque Lorsque vous activez les rapports anonymes, vous acceptez de transférer les données spécifiées à Cisco ou aux fournisseurs agissant pour le compte de Cisco (y compris dans des pays en dehors des États-Unis). Cisco protège la confidentialité de tous ses clients. Pour en savoir plus sur le traitement des renseignements personnels par Cisco, consultez la Déclaration de confidentialité de Cisco à l'adresse suivante : http://www.cisco.com/web/siteassets/legal/privacy.html

Lorsque l'ASA configure les rapports anonymes de Smart Call Home en arrière-plan, l'ASA crée automatiquement un point de confiance contenant le certificat de la CA qui émet le certificat de serveur Call Home. L'ASA prend désormais en charge la validation du certificat si la hiérarchie d'émission du certificat de serveur change, sans avoir besoin de l'intervention du client pour apporter des modifications à la hiérarchie des certificats. Vous pouvez également importer automatiquement les certificats du groupe de confiance afin que l'ASA renouvelle la hiérarchie des certificats sans intervention manuelle.

Lorsque vous mettez à niveau ASA 9.14(2.14), la configuration du point de confiance passe automatiquement de CallHome_ServerCA à CallHome_ServerCA2.

Exigence DNS

Un serveur DNS doit être configuré correctement pour que l'ASA atteigne le serveur Cisco Smart Call Home et envoie des messages à Cisco. Comme il est possible que l'ASA réside dans un réseau privé et n'ait pas accès au réseau public, Cisco vérifie votre configuration DNS puis la configure pour vous, au besoin, en procédant comme suit :

1. Effectuer une recherche DNS pour tous les serveurs DNS configurés.
2. Obtenir le serveur DNS à partir du serveur DHCP en envoyant des messages DHCPINFORM sur l'interface du niveau de sécurité le plus élevé.
3. Utiliser les serveurs DNS de Cisco pour la recherche.
4. Utiliser des adresses IP statiques de façon aléatoire pour tools.cisco.com.

Ces tâches sont effectuées sans modifier la configuration actuelle. (Par exemple, le serveur DNS appris à partir du DHCP ne sera pas ajouté à la configuration.)

Si aucun serveur DNS n'est configuré et que l'ASA ne peut pas atteindre le serveur Cisco Smart Call Home, Cisco génère un message de journal système avec le niveau de gravité d'avertissement pour chaque message Smart Call Home envoyé pour vous rappeler de configurer le DNS correctement.

Consultez le guide des messages de journal système pour obtenir des renseignements sur les messages de journal système.

À propos de Smart Call Home

Une fois entièrement configuré, Smart Call Home détecte les problèmes sur votre site et les signale à Cisco ou par l'intermédiaire d'autres canaux définis par l'utilisateur (comme la messagerie électronique ou directement), souvent avant même que vous ne soyez conscient de l'existence de ces problèmes. Selon la gravité de ces problèmes, Cisco répond à vos problèmes de configuration système, à vos annonces de fin de vie de produit, à vos problèmes d'avis de sécurité, etc. en fournissant les services suivants :

- Identification rapide des problèmes grâce à une surveillance continue, des alertes proactives en temps réel et des diagnostics détaillés.
- Signalement des problèmes potentiels grâce aux notifications Smart Call Home, dans lesquelles une demande de service a été ouverte, avec toutes les données de diagnostic jointes.
- Résolution plus rapide des problèmes critiques grâce à un accès direct et automatique aux experts du TAC de Cisco.
- Utilisation plus efficace des ressources en personnel grâce à une résolution de problèmes plus rapide.
- Génération automatique des demandes de service auprès du TAC de Cisco (si vous disposez d'un contrat de service), acheminées vers l'équipe d'assistance appropriée, qui fournit des renseignements détaillés à propos du diagnostic permettant d'accélérer la résolution des problèmes.

Le portail Smart Call Home offre un accès rapide aux renseignements requis qui vous permettent d'effectuer les opérations suivantes :

- Passer en revue tous les messages, les diagnostics et les recommandations de Smart Call Home en un seul endroit.
- Vérifier l'état des demandes de service.
- Consulter les renseignements les plus récents sur l'inventaire et la configuration de tous les appareils compatibles avec Smart Call Home.

Lignes directrices relatives aux rapports anonymes et à Smart Call Home

Cette section comprend des lignes directrices et des limites que vous devez consulter avant de configurer les rapports anonymes et Smart Call Home.

Lignes directrices relatives aux rapports anonymes

- Le DNS doit être configuré.
- Si un message de rapport anonyme ne peut pas être envoyé lors du premier essai, l'ASA réessaie deux fois avant d'abandonner le message.
- Les rapports anonymes peuvent coexister avec d'autres configurations de Smart Call Home sans modifier la configuration existante. Par exemple, si Smart Call Home est désactivé avant d'activer la création de rapports anonymes, il reste désactivé, même après l'activation des rapports anonymes.
- Si les rapports anonymes sont activés, vous ne pouvez pas supprimer le point de confiance, et lorsque les rapports anonymes sont désactivés, le point de confiance reste. Si les rapports anonymes sont désactivés, vous pouvez supprimer le point de confiance, mais la désactivation des rapports anonymes n'entraînera pas la suppression du point de confiance.
- Si vous utilisez une configuration en mode de contexte multiple, les commandes **dns**, **interface** et **trustpoint** sont dans le contexte d'administration et les commandes **call-home** sont dans le contexte système.

- Vous pouvez automatiser la mise à jour de l'ensemble de groupes de confiance à des intervalles périodiques afin que Smart Call Home puisse rester actif si le certificat autosigné du serveur CA change. Cette fonctionnalité de renouvellement automatique des groupes de confiance n'est pas prise en charge dans le cadre des déploiements à contextes multiples.

Lignes directrices relatives à Smart Call Home

- En mode de contexte multiple, la commande subscribe-to-alert-group snapshot periodic est divisée en deux commandes : l'une pour obtenir des renseignements de la configuration système et l'autre pour obtenir des renseignements du contexte utilisateur.
- Le serveur dorsal Smart Call Home n'accepte que les messages au format XML.
- Un message Smart Call Home est envoyé à Cisco pour signaler des événements de grappe importants si vous avez activé la mise en grappe et configuré Smart Call Home pour vous abonner au groupe d'alertes de diagnostic avec un niveau de gravité critique. Un message de mise en grappe Smart Call Home est envoyé uniquement pour les événements suivants :
  - Lorsqu'une unité rejoint la grappe
  - Lorsqu'une unité quitte la grappe
  - Lorsqu'une unité de grappe devient l'unité de contrôle de grappe
  - Lorsqu'une unité secondaire tombe en panne dans la grappe

  Chaque message envoyé comprend les renseignements suivants :
  - Le nombre de membres actifs dans la grappe
  - La sortie de la commande **show cluster info** et de la commande **show cluster history** sur l'unité de contrôle de grappe

Configurer les rapports anonymes et Smart Call Home

Les rapports anonymes font partie du service Smart Call Home et permettent à Cisco de recevoir de manière anonyme un minimum de renseignements sur les erreurs et l'intégrité de votre appareil, mais le service Smart Call Home offre une assistance personnalisée sur l'intégrité de votre système, ce qui permet au TAC de Cisco de superviser vos appareils et d'ouvrir un dossier lorsqu'il y a un problème, souvent avant même que vous sachiez que le problème est survenu.

Vous pouvez avoir les deux services configurés sur votre système en même temps, bien que la configuration du service Smart Call Home offre les mêmes fonctionnalités que les rapports anonymes, ainsi que des services personnalisés.

Configurer les rapports anonymes

Pour configurer les rapports anonymes, procédez comme suit.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call Home**.

Étape 2 Cochez la case **Enable Anonymous Reporting** (Activer les rapports anonymes).

Étape 3 Cliquez sur **Test Connection** (Tester la connexion) pour vous assurer que votre système est en mesure d'envoyer des messages.

ASDM renvoie un message de réussite ou d'erreur pour vous informer des résultats du test.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer la configuration et activer les rapports anonymes.

Configurer Smart Call Home

Pour configurer le service Smart Call Home, la configuration système et les profils d'abonnement aux alertes, procédez comme suit.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call Home**.

Étape 2 Cochez la case **Enable Registered Smart Call Home** (Activer le Smart Call Home enregistré) pour activer Smart Call Home et enregistrer votre ASA auprès du TAC de Cisco.

Étape 3 Cliquez deux fois sur **Advanced System Setup** (Configuration système avancée). Cette zone se compose de trois volets. Chaque volet peut être développé ou réduit en cliquant deux fois sur la ligne de titre.

a) Vous pouvez configurer des serveurs de messagerie dans le volet **Mail Servers** (Serveurs de messagerie), par lequel les messages Smart Call Home sont envoyés aux abonnés par courriel.

b) Vous pouvez saisir les renseignements de la personne-ressource dans le volet **Contact Information** (Coordonnées) pour l'ASA qui s'affiche dans les messages de Smart Call Home. Ce volet comprend les renseignements suivants :

- Le nom de la personne-ressource.
- Le numéro de téléphone de la personne-ressource.
- L'adresse postale de la personne-ressource.
- L'adresse courriel de la personne-ressource.
- L'adresse courriel « expéditeur » dans le courriel de Smart Call Home.
- L'adresse courriel « répondre à » dans le courriel de Smart Call Home.
- L'ID du client.
- L'ID du site.
- L'ID de contrat.

c) Vous pouvez ajuster les paramètres de contrôle des alertes dans le volet **Alert Control** (Contrôle des alertes). Ce volet comprend le volet **Alert Group Status** (État du groupe d'alertes), qui répertorie l'état (activé ou désactivé) des groupes d'alertes suivants :

- Le groupe d'alertes de diagnostic.
- Le groupe d'alertes de configuration.
- Le groupe d'alertes d'environnement.
- Le groupe d'alertes d'inventaire.
- Le groupe d'alertes d'instantané.
- Le groupe d'alertes de journal système.
- Le groupe d'alertes de télémétrie.
- Le groupe d'alertes de menace.
- Le nombre maximum de messages Smart Call Home traités par minute.
- L'adresse courriel « expéditeur » dans le courriel de Smart Call Home.

Étape 4 Cliquez deux fois sur **Alert Subscription Profiles** (Profils d'abonnement aux alertes). Chaque profil d'abonnement nommé identifie les abonnés et les groupes d'alertes d'intérêt.

a) Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour afficher le **Subscription Profile Editor** (Éditeur de profil d'abonnement), dans lequel vous pouvez créer un nouveau profil d'abonnement ou modifier un profil d'abonnement existant.
b) Cliquez sur **Delete** (Supprimer) pour supprimer le profil sélectionné.
c) Cochez la case **Active** (Actif) pour envoyer un message Smart Call Home du profil d'abonnement sélectionné aux abonnés.

Étape 5 Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour afficher la boîte de dialogue **Add** (Ajouter) ou **Edit Alert Subscription Profile** (Modifier le profil d'abonnement aux alertes).

a) Le champ **Name** (Nom) est en lecture seule et ne peut pas être modifié.
b) Cochez la case **Enable this subscription profile** (Activer ce profil d'abonnement) pour activer ou désactiver ce profil en particulier.
c) Cliquez sur le bouton radio **HTTP** ou **Email** (Courriel) dans la zone **Alert Delivery Method** (Méthode de distribution d'alertes).
d) Saisissez l'adresse courriel ou l'adresse Web dans le champ **Subscribers** (Abonnés).
e) Spécifiez un objet **Reference Identity** (Identité de référence) par nom pour activer les vérifications d'identité de référence RFC 6125 sur le certificat reçu du serveur de journal système.

   Consultez Configurer les identités de référence, à la page 828 pour en savoir plus sur l'objet d'identité de référence.

Étape 6 La zone **Alert Dispatch** (Envoi d'alertes) permet à l'administrateur de préciser le type de renseignements Smart Call Home à envoyer aux abonnés et dans quelles conditions. Il existe deux types d'alertes, basées sur le temps et basées sur des événements, choisies en fonction de la façon dont l'alerte est déclenchée. Les groupes d'alertes suivants sont à baser sur le temps : configuration, inventaire, instantané et télémétrie. Les groupes d'alertes suivants sont basés sur des événements : diagnostic, environnement, journal système et menace.

Étape 7 La zone **Message Parameters** (Paramètres de message) vous permet d'ajuster les paramètres qui contrôlent les messages envoyés à l'abonné, y compris le format de message préféré et la taille de message maximum.

Étape 8 Pour les alertes basées sur le temps, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Add** (Ajouter) ou **Edit Configuration Alert Dispatch Condition** (Modifier une condition d'envoi d'alertes de configuration).

a) Spécifiez la fréquence dans le champ **Alert Dispatch Frequency** (Fréquence d'envoi d'alertes) à laquelle envoyer les renseignements aux abonnés :

- Pour un abonnement mensuel, indiquez le jour du mois et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement hebdomadaire, indiquez le jour de la semaine et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement quotidien, indiquez l'heure du jour pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée.
- Pour un abonnement horaire, indiquez la minute de l'heure pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée. Les abonnements horaires s'appliquent uniquement aux groupes d'alertes d'instantané et de télémétrie.

b) Cliquez sur le bouton radio **Basic** (De base) ou **Detailed** (Détaillé) pour fournir le niveau de renseignements souhaité aux abonnés.

c) Cliquez sur **OK** pour enregistrer la configuration

Étape 9 Pour les alertes de diagnostic, d'environnement et de menace, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Create** (Créer) ou **Edit Diagnostic Alert Dispatch Condition** (Modifier une condition d'envoi d'alerte de diagnostic).

Étape 10 Précisez la gravité de l'événement qui déclenche l'envoi de l'alerte aux abonnés dans la liste déroulante **Event Severity** (Gravité de l'événement), puis cliquez sur **OK**.

Étape 11 Pour les alertes basées sur le temps d'inventaire, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Create** (Créer) ou **Edit Inventory Alert Dispatch Condition** (Modifier une condition d'envoi d'alerte d'inventaire).

Étape 12 Précisez la fréquence d'envoi des alertes aux abonnés dans la liste déroulante **Alert Dispatch Frequency** (Fréquence d'envoi des alertes), puis cliquez sur **OK**.

Étape 13 Pour les alertes basées sur le temps d'instantané, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Create** (Créer) ou **Edit Snapshot Alert Dispatch Condition** (Modifier une condition d'envoi d'alerte d'instantané).

a) Spécifiez la fréquence dans le champ **Alert Dispatch Frequency** (Fréquence d'envoi d'alertes) à laquelle envoyer les renseignements aux abonnés :

- Pour un abonnement mensuel, indiquez le jour du mois et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement hebdomadaire, indiquez le jour de la semaine et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement quotidien, indiquez l'heure du jour pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée.
- Pour un abonnement horaire, indiquez la minute de l'heure pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée. Les abonnements horaires s'appliquent uniquement aux groupes d'alertes d'instantané et de télémétrie.

- Pour un intervalle d'abonnement, indiquez la fréquence en minutes à laquelle les renseignements doivent être envoyés aux abonnés. Cette exigence s'applique uniquement au groupe d'alertes d'instantané.

b) Cliquez sur **OK** pour enregistrer la configuration

Étape 14 Pour les alertes basées sur des événements de journal système, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Create** (Créer) ou **Edit Syslog Alert Dispatch Condition** (Modifier une condition d'envoi d'alerte de journal système).

a) Cochez la case **Specify the event severity which triggers the dispatch of alert to subscribers** (Spécifier la gravité de l'événement qui déclenche l'envoi de l'alerte aux abonnées), et choisissez la gravité de l'événement dans la liste déroulante.

b) Cochez la case **Specify the message IDs of syslogs which trigger the dispatch of alert to subscribers** (Spécifier les ID de message des journaux système qui déclenchent l'envoi de l'alerte aux abonnés).

c) Spécifiez les ID de message des journaux système qui déclenchent l'envoi de l'alerte aux abonnés en fonction des instructions à l'écran.

d) Cliquez sur **OK** pour enregistrer la configuration

Étape 15 Pour les alertes basées sur des événements de télémétrie, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Create** (Créer) ou **Edit Telemetry Alert Dispatch Condition** (Modifier une condition d'envoi d'alerte de télémétrie).

a) Spécifiez la fréquence dans le champ **Alert Dispatch Frequency** (Fréquence d'envoi d'alertes) à laquelle envoyer les renseignements aux abonnés :

- Pour un abonnement mensuel, indiquez le jour du mois et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement hebdomadaire, indiquez le jour de la semaine et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement quotidien, indiquez l'heure du jour pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée.
- Pour un abonnement horaire, indiquez la minute de l'heure pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée. Les abonnements horaires s'appliquent uniquement aux groupes d'alertes d'instantané et de télémétrie.

b) Cliquez sur **OK** pour enregistrer la configuration

Étape 16 Cliquez sur **Test** (Tester) pour déterminer si les alertes configurées fonctionnent correctement.

Configurer l'importation automatique des certificats de groupe de confiance

La licence Smart utilise l'infrastructure Smart Call Home. Lorsque l'ASA configure les rapports anonymes de Smart Call Home en arrière-plan, l'ASA crée automatiquement un point de confiance contenant le certificat de la CA qui a émis le certificat de serveur Call Home. L'ASA prend désormais en charge la validation du certificat si la hiérarchie d'émission du certificat de serveur change, sans avoir besoin de l'intervention du client pour ajuster les modifications à la hiérarchie des certificats. Vous pouvez automatiser la mise à jour de l'ensemble de groupes de confiance à des intervalles périodiques afin que Smart Call Home puisse rester actif si le certificat autosigné du serveur CA change. Cette fonctionnalité n'est pas prise en charge dans le cadre des déploiements à contextes multiples.

L'importation automatique des ensembles de certificat de confiance vous oblige à spécifier l'URL utilisée par l'ASA pour télécharger et importer le groupe. Utilisez la commande suivante pour que l'importation ait lieu quotidiennement à des intervalles réguliers avec l'URL Cisco par défaut et l'heure par défaut de 22 heures :

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

Vous pouvez également activer l'importation automatique avec une URL personnalisée à l'aide de la commande suivante :

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

Pour vous offrir plus de flexibilité pour définir les téléchargements en dehors des heures de pointe ou à d'autres moments pratiques, saisissez la commande suivante qui active l'importation avec une heure personnalisée :

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

La définition de l'importation automatique avec une URL personnalisée et une heure personnalisée nécessite la commande suivante :

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

Supervision des rapports anonymes et de Smart Call Home

Consultez les commandes suivantes pour superviser les services de création de rapports anonymes et les services Smart Call Home. Vous pouvez saisir ces commandes en sélectionnant **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**.

- **show call-home detail**

  Cette commande affiche la configuration détaillée de Smart Call Home actuelle.

- **show call-home mail-server status**

  Cette commande affiche l'état actuel du serveur de messagerie.

- **show call-home profile** {profile name | **all**}

  Cette commande affiche la configuration des profils Smart Call Home.

- **show call-home registered-module status** [**all**]

  Cette commande affiche l'état du module enregistré.

- **show call-home statistics**

  Cette commande affiche l'état détaillé de Smart Call Home.

- **show call-home**

  Cette commande affiche la configuration de Smart Call Home actuelle.

- **show running-config call-home**

  Cette commande affiche la configuration en cours d'exécution de Smart Call Home actuelle.

- **show smart-call-home alert-group**

  Cette commande affiche l'état actuel des groupes d'alertes Smart Call Home.

- **show running-config all**

  Cette commande affiche les détails du profil d'utilisateur des rapports anonymes.

Historique des rapports anonymes et de Smart Call Home

Tableau 73 : Historique des rapports anonymes et de Smart Call Home

Nom de la caractéristique	Versions de plateforme	Description
Smart Call Home	8.2(2)	Le service Smart Call Home offre des diagnostics proactifs et des alertes en temps réel sur l'ASA, et assure une meilleure disponibilité du réseau et une efficacité opérationnelle accrue. Nous avons introduit l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Smart Call Home.
Rapports anonymes	9.0(1)	Vous pouvez contribuer à l'amélioration de la plateforme ASA en activant les rapports anonymes, qui permettent à Cisco de recevoir en toute sécurité un minimum de renseignements sur les erreurs et l'intégrité d'un appareil. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Smart Call Home.
Smart Call Home	9.1(2)	La commande **show local-host** a été remplacée par la commande **show local-host | include interface** pour la création de rapports sur les groupes d'alertes de télémétrie.
Smart Call Home	9.1(3)	Un message Smart Call Home est envoyé à Cisco pour signaler des événements de grappe importants si vous avez activé la mise en grappe et configuré Smart Call Home pour vous abonner au groupe d'alertes de diagnostic avec un niveau de gravité Critique. Un message de mise en grappe Smart Call Home est envoyé uniquement pour les trois événements suivants : • Lorsqu'une unité rejoint la grappe • Lorsqu'une unité quitte la grappe • Lorsqu'une unité de grappe devient l'unité de contrôle de grappe Chaque message envoyé comprend les renseignements suivants : • Le nombre de membres actifs dans la grappe • La sortie de la commande **show cluster info** et de la commande **show cluster history** sur l'unité de contrôle de grappe

Nom de la caractéristique	Versions de plateforme	Description
Identités de référence pour les connexions sécurisées au serveur Smart Call Home	9.6(2)	Le traitement du client TLS prend désormais en charge les règles de vérification de l'identité de serveur définies dans la RFC 6125, section 6. La vérification de l'identité sera effectuée lors de la validation PKI pour les connexions TLS au serveur Smart Call Home. Si l'identité présentée ne correspond pas à l'identité de référence configurée, la connexion n'est pas établie. Nous avons modifié la page suivante : **Configuration > Device Management (Gestion des périphériques) > Smart Call Home**.



PARTIE IX

Numéro de référence

- Adresses, protocoles et ports, à la page 1351



CHAPITRE 53

Adresses, protocoles et ports

Ce chapitre fournit une référence rapide des adresses IP, des protocoles et des applications.

- Adresses IPv4 et filtres d'adresse locale, à la page 1351
- Adresses IPv6, à la page 1355
- Protocoles et applications, à la page 1361
- Ports TCP et UDP, à la page 1362
- Ports et protocoles locaux, à la page 1365
- Types ICMP, à la page 1367

Adresses IPv4 et filtres d'adresse locale

Cette section décrit comment utiliser les adresses IPv4 dans l'ASA. Une adresse IPv4 est un nombre de 32 bits écrits en notation décimale à points : quatre champs de 8 bits (octets) convertis de nombres binaires en nombres décimaux, séparés par des points. La première partie d'une adresse IP identifie le réseau sur lequel réside l'hôte, tandis que la seconde partie identifie l'hôte sur le réseau donné. Le champ de numéro de réseau s'appelle le préfixe réseau. Tous les hôtes sur un réseau donné partagent le même préfixe réseau, mais doivent avoir un numéro d'hôte unique. Dans un réseau avec des classes d'adresses IP, la classe de l'adresse détermine la limite entre le préfixe de réseau et le numéro d'hôte.

Classes

Les adresses IP des hôtes sont divisées en trois classes d'adresses différentes : la classe A, la classe B et la classe C. Chaque classe fixe la limite entre le préfixe réseau et le numéro d'hôte à un point différent dans l'adresse de 32 bits. Les adresses de classe D sont réservées à l'IP de multidiffusion.

- Les adresses de classe A (1.xxx.xxx.xxx à 126.xxx.xxx.xxx) utilisent uniquement le premier octet comme préfixe réseau.
- Les adresses de classe B (128.0.xxx.xxx à 191.255.xxx.xxx) utilisent les deux premiers octets comme préfixe réseau.
- Les adresses de classe C (192.0.0.xxx à 223.255.255.xxx) utilisent les trois premiers octets comme préfixe réseau.

Comme les adresses de classe A ont 16 777 214 adresses d'hôtes et les adresses de classe B de 65 534 hôtes, vous pouvez utiliser le filtrage d'adresse locale pour diviser ces énormes réseaux en sous-réseaux plus petits.

Réseaux privés

Si vous avez besoin d'un grand nombre d'adresses sur votre réseau, et qu'elles n'ont pas besoin d'être acheminées sur Internet, vous pouvez utiliser des adresses IP privées que l'autorité d'attribution de numéros par Internet (IANA) recommande (voir RFC 1918). Les plages d'adresses suivantes sont désignées comme des réseaux privés qui ne doivent pas être annoncés :

- 10.0.0.0 à 10.255.255.255
- 172.16.0.0 à 172.31.255.255
- 192.168.0.0 à 192.168.255.255

Filtres d'adresse locale

Un filtre d'adresse locale vous permet de convertir un seul réseau de classe A, B ou C en plusieurs réseaux. Avec un filtre d'adresse locale, vous pouvez créer un préfixe de réseau étendu qui ajoute des bits du numéro d'hôte au préfixe de réseau. Par exemple, un préfixe de réseau de classe C est toujours composé des trois premiers octets de l'adresse IP. Mais un préfixe de réseau étendu de classe C utilise également une partie du quatrième octet.

Le filtrage d'adresse locale est facile à comprendre si vous utilisez la notation binaire au lieu de la notation décimale à points. Les bits du filtre d'adresse locale ont une correspondance un-à-un avec l'adresse Internet :

- Les bits sont définis sur 1 si le bit correspondant dans l'adresse IP fait partie du préfixe de réseau étendu.
- Les bits sont définis sur 0 si le bit fait partie du numéro d'hôte.

Exemple 1 : si vous avez l'adresse de classe B 129.10.0.0 et que vous souhaitez utiliser le troisième octet dans le préfixe du réseau étendu au lieu du numéro d'hôte, vous devez spécifier un filtre d'adresse locale 11111111.11111111.11111111.00000000. Ce filtre d'adresse locale convertit l'adresse de classe B en équivalent d'une adresse de classe C, où le numéro d'hôte est composé uniquement du dernier octet.

Exemple 2 : si vous souhaitez utiliser une partie du troisième octet pour le préfixe de réseau étendu, vous devez préciser un filtre d'adresse locale comme 11111111.11111111.11111000.00000000, qui utilise seulement 5 bits du troisième octet pour le préfixe de réseau étendu.

Vous pouvez écrire un filtre d'adresse locale sous forme de masque décimal à points ou de masque /*bits* (« barre oblique *bits* »). Dans l'exemple 1, pour un masque décimal à points, vous convertissez chaque octet binaire en un nombre décimal : 255.255.255.0. Pour un masque /*bits*, vous ajoutez le nombre de 1 : /24. Dans l'exemple 2, le nombre décimal est 255.255.248.0 et le /bits est /21.

Vous pouvez également regrouper plusieurs réseaux de classe C dans un réseau plus vaste en utilisant une partie du troisième octet pour le préfixe de réseau étendu. Par exemple, 192.168.0.0/20.

Déterminer le filtre d'adresse locale

Consultez le tableau suivant pour déterminer le filtre d'adresse locale en fonction du nombre d'hôtes souhaité.



Remarque Le premier et le dernier numéro d'un sous-réseau sont réservés, à l'exception de /32, qui identifie un seul hôte.

Tableau 74 : Hôtes, bits et masques décimaux à points

Hôtes	/Masque de bits	Masque décimal à points
16,777,216	/8	Réseau de classe A 255.0.0.0
65,536	/16	Réseau de classe B 255.255.0.0
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	Réseau de classe C 255.255.255.0
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
Ne pas utiliser	/31	255.255.255.254
1	/32	Adresse d'hôte unique 255.255.255.255

Déterminer l'adresse à utiliser avec le filtre d'adresse locale

Les sections suivantes décrivent comment déterminer l'adresse réseau à utiliser avec un filtre d'adresse locale pour un réseau de classe C et de classe B.

Adresse réseau de classe C

Pour un réseau compris entre 2 et 254 hôtes, le quatrième octet tombe sur un multiple du nombre d'adresses d'hôte, en commençant par 0. Par exemple, le tableau suivant montre les sous-réseaux de 8 hôtes (/29) de 192.168.0.x.

Remarque La première et la dernière adress d'un sous-réseau sont réservées. Dans le premier exemple de sous-réseau, vous ne pouvez pas utiliser 192.168.0.0 ou 192.168.0.7.

Tableau 75 : Adresse réseau de classe C

Sous-réseau avec le masque /29 (255.255.255.248)	Plage d'adresses
192.168.0.0	De 192.168.0.0 à 192.168.0.7
192.168.0.8	De 192.168.0.8 à 192.168.0.15
192.168.0.16	De 192.168.0.16 à 192.168.0.31
—	—
192.168.0.248	De 192.168.0.248 à 192.168.0.255

Adresse réseau de classe B

Pour déterminer l'adresse réseau à utiliser avec le filtre d'adresse locale pour un réseau de 254 à 65 534 hôtes, vous devez déterminer la valeur du troisième octet pour chaque préfixe de réseau étendu possible. Par exemple, vous pouvez créer une adresse de sous-réseau comme 10.1.*x*.0, où les deux premiers octets sont fixes, car ils sont utilisés dans le préfixe de réseau étendu, et le quatrième octet est 0, car tous les bits sont utilisés pour le numéro d'hôte.

Pour déterminer la valeur du troisième octet, procédez comme suit :

1. Calculez le nombre de sous-réseaux que vous pouvez créer à partir du réseau en divisant 65 536 (le nombre total d'adresses en utilisant le troisième et le quatrième octet) par le nombre d'adresses d'hôtes souhaitées.

   Par exemple, 65 536 divisés par 4 096 hôtes équivaut à 16. Par conséquent, il existe 16 sous-réseaux de 4 096 adresses chacun dans un réseau de classe B.

2. Déterminez le multiple de la valeur du troisième octet en divisant 256 (le nombre de valeurs pour le troisième octet) par le nombre de sous-réseaux :

   Dans cet exemple, 256/16 = 16.

   Le troisième octet correspond à un multiple de 16, commençant par 0.

Le tableau suivant présente les 16 sous-réseaux du réseau 10.1.

Remarque La première et la dernière adress d'un sous-réseau sont réservées. Dans le premier exemple de sous-réseau, vous ne pouvez pas utiliser 10.1.0.0 ou 10.1.15.255.

Tableau 76 : Sous-réseaux du réseau

Sous-réseau avec le masque /20 (255.255.240.0)	Plage d'adresses
10/100	De 10.1.0.0 à 10.1.15.255
10.1.16.0	De 10.1.16.0 à 10.1.31.255
10.1.32.0	De 10.1.32.0 à 10.1.47.255
—	—

Sous-réseau avec le masque /20 (255.255.240.0)	Plage d'adresses
10.1.240.0	De 10.1.240.0 à 10.1.255.255

Adresses IPv6

IPv6 est la prochaine génération de protocole Internet après IPv4. Il fournit un espace d'adressage étendu, un format d'en-tête simplifié, une prise en charge améliorée des extensions et des options, une capacité d'étiquetage des flux, ainsi que des capacités d'authentification et de confidentialité. IPv6 est décrit dans la RFC 2460. L'architecture d'adressage IPv6 est décrite dans la RFC 3513.

Cette section décrit le format et l'architecture de l'adresse IPv6.

Format d'adresses IPv6

Les adresses IPv6 sont représentées par une série de huit champs hexadécimaux de 16 bits séparés par des deux-points (:) au format : x:x:x:x:x:x:x:x. Voici deux exemples d'adresses IPv6 :

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

Remarque Les lettres hexadécimales dans les adresses IPv6 ne sont pas sensibles à la casse.

Vous n'avez pas besoin d'inclure les zéros initiaux dans un champ individuel de l'adresse, mais chaque champ doit contenir au moins un chiffre. Ainsi, l'exemple d'adresse 2001:0DB8:0000:0000:0008:0800:200C:417A peut être raccourci à 2001:0DB8:0:0:8:800:200C:417A en supprimant les zéros initiaux du troisième au cinquième champ à partir de la gauche. Les champs qui contiennent tous des zéros (les troisième et quatrième champs à partir de la gauche) ont été raccourcis à un seul zéro. Les trois zéros initiaux ont été supprimés dans le cinquième champ à partir de la gauche, ce qui a laissé un seul 8 dans ce champ, et le zéro initial a été supprimé dans le sixième champ à partir de la gauche, laissant 800 dans ce champ.

Il est courant que les adresses IPv6 contiennent plusieurs champs hexadécimaux consécutifs de zéros. Vous pouvez utiliser deux signes de deux-points (::) pour compresser des champs consécutifs de zéros au début, au milieu ou à la fin d'une adresse IPv6 (les deux-points représentent les champs hexadécimaux successifs de zéros). Le tableau suivant présente plusieurs exemples de compression d'adresses pour différents types d'adresses IPv6.

Tableau 77 : Exemples de compression d'adresses IPv6

Type d'adresse	Forme standard	Forme compressée
Monodiffusion	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
Multicast (multidiffusion)	FF01:0:0:0:0:0:0:101	FF01::101
Boucle avec retour	0:0:0:0:0:0:0:1	::1

Type d'adresse	Forme standard	Forme compressée
Non défini	0:0:0:0:0:0:0:0	::

Remarque Deux signes de deux-points (::) ne peuvent être utilisés qu'une seule fois dans une adresse IPv6 pour représenter des champs successifs de zéros.

Une autre forme du format IPv6 est souvent utilisée lorsqu'il s'agit d'un environnement contenant des adresses IPv4 et IPv6. Cette alternative a le format x:x:x:x:x:x:y.y.y.y, où x représente les valeurs hexadécimales des six parties de l'adresse IPv6 et y représente les valeurs décimales de la partie IPv4 de 32 bits de l'adresse (qui prend la place des deux autres parties de 16 bits de l'adresse IPv6). Par exemple, l'adresse IPv4 192.168.1.1 pourrait être représentée comme l'adresse IPv6 0:0:0:0:0:0:FFFF:192.168.1.1 ou ::FFFF:192.168.1.1.

Types d'adresses IPv6

Les trois principaux types d'adresses IPv6 sont les suivants :

- **Monodiffusion** : une adresse de monodiffusion est un identifiant pour une seule interface. Un paquet envoyé à une adresse de monodiffusion est livré à l'interface identifiée par cette adresse. Une interface peut avoir plusieurs adresses de monodiffusion.
- **Multidiffusion** : une adresse de multidiffusion est un identifiant pour un ensemble d'interfaces. Un paquet envoyé à une adresse de multidiffusion est transmis à toutes les adresses identifiées par cette adresse.
- **Anycast** : une adresse Anycast est un identifiant pour un ensemble d'interfaces. Contrairement à une adresse de multidiffusion, un paquet envoyé à une adresse Anycast n'est livré qu'à l'interface « la plus proche », comme déterminé par la mesure des distances pour le protocole de routage.

Remarque Il n'y a pas d'adresses de diffusion dans IPv6. Les adresses de multidiffusion fournissent la fonctionnalité de diffusion.

Adresses de monodiffusion

Cette section décrit les adresses de monodiffusion IPv6. Les adresses de monodiffusion identifient une interface sur un nœud de réseau.

Adresse globale

Le format général d'une adresse de monodiffusion globale IPv6 est un préfixe de routage global suivi d'un ID de sous-réseau suivi d'un ID d'interface. Le préfixe de routage global peut être n'importe quel préfixe non réservé par un autre type d'adresse IPv6.

Toutes les adresses de monodiffusion globales, hormis celles commençant par le binaire 000, ont un ID d'interface de 64 bits au format EUI-64 modifié.

Les adresses de monodiffusion globales commençant par le binaire 000 n'ont aucune contrainte quant à la taille ou à la structure de la partie ID d'interface de l'adresse. Un exemple de ce type d'adresse est une adresse IPv6 avec une adresse IPv4 intégrée.

Adresse Site-Local

Les adresses Site-Local sont utilisées pour l'adressage au sein d'un site. Elles peuvent être utilisées pour traiter un site entier sans utiliser de préfixe globalement unique. Les adresses Site-Local ont le préfixe FEC0::/10, suivi d'un ID de sous-réseau de 54 bits, et se terminent par un ID d'interface de 64 bits au format EUI-64 modifié.

Les routeurs Site-Local ne transfèrent pas les paquets qui ont une adresse Site-Local pour une source ou une destination à l'extérieur du site. Par conséquent, les adresses Site-Local peuvent être considérées comme des adresses privées.

Adresse Link-Local

Toutes les interfaces doivent avoir au moins une adresse Link-Local. Vous pouvez configurer plusieurs adresses IPv6 par interface, mais une seule adresse Link-Local.

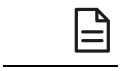
Une adresse Link-Local est une adresse de monodiffusion IPv6 qui peut être configurée automatiquement sur n'importe quelle interface à l'aide du préfixe de lien local FE80::/10 et de l'identifiant d'interface au format EUI-64 modifié. Les adresses Link-Local sont utilisées dans le protocole de découverte de voisin et dans le processus de configuration automatique sans état. Les nœuds ayant une adresse Link-Local peuvent communiquer; ils n'ont pas besoin d'une adresse locale au site ou d'une adresse unique au niveau mondial pour communiquer.

Les routeurs ne transfèrent pas les paquets qui ont une adresse Link-Local pour un contrôleur source ou de destination. Par conséquent, les adresses Link-Local peuvent être considérées comme des adresses privées.

Adresses IPv6 compatibles avec IPv4

Il existe deux types d'adresses IPv6 qui peuvent contenir des adresses IPv4.

Le premier type est l'adresse IPv6 compatible avec IPv4. Les mécanismes de transition IPv6 comprennent une technique permettant aux hôtes et aux routeurs de tunneler de manière dynamique les paquets IPv6 sur l'infrastructure de routage IPv4. Les nœuds IPv6 qui utilisent cette technique se voient attribuer des adresses de monodiffusion IPv6 spéciales qui transportent une adresse IPv4 globale dans les 32 bits de poids faible. Ce type d'adresse est appelé adresse IPv6 compatible avec IPv4 et a le format ::y.y.y.y, où y.y.y.y est une adresse de monodiffusion IPv4.



Remarque L'adresse IPv4 utilisée dans l'adresse IPv6 compatible avec IPv4 doit être une adresse de monodiffusion IPv4 globalement unique.

Le deuxième type d'adresse IPv6, qui contient une adresse IPv4 intégrée, s'appelle l'adresse IPv6 mappée en IPv4. Ce type d'adresse est utilisé pour représenter les adresses des nœuds IPv4 en tant qu'adresses IPv6. Ce type d'adresse est au format ::FFFF:y.y.y.y, où y.y.y.y est une adresse de monodiffusion IPv4.

Adresse non spécifiée

L'adresse non spécifiée, 0:0:0:0:0:0:0:0, indique l'absence d'adresse IPv6. Par exemple, un nœud nouvellement initialisé sur un réseau IPv6 peut utiliser l'adresse non spécifiée comme adresse source dans ses paquets jusqu'à ce qu'il reçoive son adresse IPv6.

Remarque L'adresse IPv6 non spécifiée ne peut pas être attribuée à une interface. Les adresses IPv6 non spécifiées ne doivent pas être utilisées comme adresses de destination dans les paquets IPv6 ou dans l'en-tête de routage IPv6.

Adresse de la boucle avec retour

L'adresse de boucle avec retour, 0:0:0:0:0:0:0:1, peut être utilisée par un nœud pour s'envoyer un paquet IPv6. L'adresse de boucle avec retour dans IPv6 fonctionne de la même manière que l'adresse de boucle avec retour dans IPv4 (127.0.0.1).

Remarque L'adresse de boucle avec retour IPv6 ne peut pas être attribuée à une interface physique. Un paquet qui a l'adresse de boucle avec retour IPv6 comme adresse source ou de destination doit rester dans le nœud qui a créé le paquet. Les routeurs IPv6 ne transfèrent pas les paquets qui ont l'adresse de boucle avec retour IPv6 comme adresse source ou de destination.

Identifiants de l'interface

Les identifiants d'interface dans les adresses de monodiffusion IPv6 sont utilisés pour identifier les interfaces sur une liaison. Ils doivent être uniques dans un préfixe de sous-réseau. Dans de nombreux cas, l'identifiant d'interface est dérivé de l'adresse de la couche de liaison de l'interface. Le même identifiant d'interface peut être utilisé sur plusieurs interfaces d'un seul nœud, tant que ces interfaces sont associées à des sous-réseaux différents.

Pour toutes les adresses de monodiffusion, à l'exception de celles qui commencent par le binaire 000, l'identifiant d'interface doit comporter 64 bits et être généré au format EUI-64 modifié. Le format EUI-64 modifié est créé à partir de l'adresse MAC de 48 bits en inversant le bit universel/local dans l'adresse et en insérant le numéro hexadécimal FFFE entre les trois octets supérieurs et les trois octets inférieurs de l'adresse MAC.

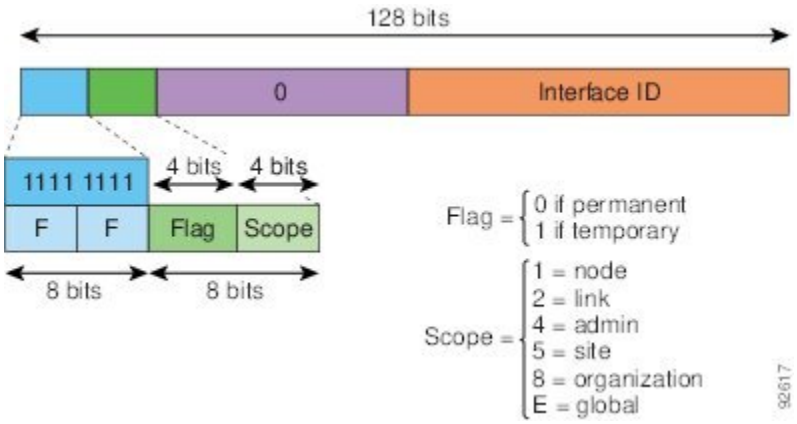
Par exemple, une interface ayant l'adresse MAC 00E0.b601.3B7A aura un ID d'interface de 64 bits 02E0:B6FF:FE01:3B7A.

Multicast Address (Adresse multidiffusion)

Une adresse de multidiffusion IPv6 est un identifiant pour un groupe d'interfaces, généralement sur des nœuds différents. Un paquet envoyé à une adresse de multidiffusion est transmis à toutes les interfaces identifiées par l'adresse de multidiffusion. Une interface peut appartenir à un nombre illimité de groupes de multidiffusion.

Une adresse de multidiffusion IPv6 a un préfixe FF00::/8 (1111 1111). L'octet suivant le préfixe définit le type et la portée de l'adresse de multidiffusion. Une adresse de multidiffusion attribuée de façon permanente (bien connue) a un paramètre d'indicateur égal à 0; une adresse de multidiffusion temporaire (transitoire) a un paramètre d'indicateur égal à 1. Une adresse de multidiffusion qui a la portée d'un nœud, d'une liaison, d'un site ou d'une organisation, ou une portée globale, a un paramètre de portée de 1, 2, 5, 8 ou E, respectivement. Par exemple, une adresse de multidiffusion avec le préfixe FF02::/16 est une adresse de multidiffusion permanente avec une portée de liaison. La figure suivante montre le format d'adresse de multidiffusion IPv6.

Illustration 98 : Format d'adresse de multidiffusion IPv6



Les nœuds IPv6 (hôtes et routeurs) doivent se joindre aux groupes de multidiffusion suivants :

- Les adresses de multidiffusion de tous les nœuds :
  - FF01:: (interface locale)
  - FF02:: (liaison locale)
- L'adresse du nœud sollicité pour chaque adresse de monodiffusion IPv6 et toute adresse Anycast sur le nœud : FF02:0:0:0:0:1:FFXX:XXXX/104, où XX:XXXX correspond aux 24 bits de poids faible de l'adresse de monodiffusion ou de l'adresse Anycast.

Remarque Les adresses de nœud sollicité sont utilisées dans les messages de demande de voisin.

Les routeurs IPv6 doivent se joindre aux groupes de multidiffusion suivants :

- FF01::2 (interface locale)
- FF02::2 (liaison locale)
- FF05::2 (site local)

L'adresse de multidiffusion ne doit pas être utilisée comme adresses source dans les paquets IPv6.

Remarque Il n'y a pas d'adresses de diffusion dans IPv6. Les adresses de multidiffusion IPv6 sont utilisées à la place des adresses de diffusion.

Adresse Anycast

L'adresse Anycast IPv6 est une adresse de monodiffusion attribuée à plusieurs interfaces (appartenant généralement à des nœuds différents). Un paquet qui est acheminé vers une adresse Anycast est acheminé

vers l'interface la plus proche ayant cette adresse, la proximité étant déterminée par le protocole de routage en vigueur.

Les adresses Anycast sont attribuées à partir de l'espace d'adressage de monodiffusion. Une adresse Anycast est simplement une adresse de monodiffusion qui a été attribuée à plusieurs interfaces, et les interfaces doivent être configurées pour reconnaître l'adresse comme une adresse Anycast.

Les restrictions suivantes s'appliquent aux adresses Anycast :

- Une adresse Anycast ne peut pas être utilisée comme adresse source pour un paquet IPv6.
- Une adresse Anycast ne peut pas être attribuée à un hôte IPv6; elle ne peut être attribuée qu'à un routeur IPv6.



Remarque Les adresses Anycast ne sont pas prises en charge sur l'ASA.

Adresses requises

Les hôtes IPv6 doivent au moins être configurés avec les adresses suivantes (automatiquement ou manuellement) :

- Une adresse Link-Local pour chaque interface
- L'adresse de boucle avec retour
- Les adresses de multidiffusion de tous les nœuds
- Une adresse de multidiffusion de nœud sollicité pour chaque adresse de monodiffusion ou Anycast

Les routeurs IPv6 doivent au moins être configurés avec les adresses suivantes (automatiquement ou manuellement) :

- Les adresses d'hôte requises
- Les adresses Anycast du routeur de sous-réseau pour toutes les interfaces pour lesquelles il est configuré pour agir en tant que routeur
- Les adresses de multidiffusion de tous les routeurs

Préfixes de l'adresse IPv6

Un préfixe d'adresse IPv6, au format ipv6-prefix/prefix-length, peut être utilisé pour représenter les blocs contigus de bit de l'ensemble de l'espace d'adressage. Le préfixe IPv6 doit être sous la forme documentée dans la RFC 2373, où l'adresse est spécifiée en format hexadécimal en utilisant des valeurs de 16 bits entre les deux-points. La longueur du préfixe est une valeur décimale qui indique le nombre de bits contigus de poids fort de l'adresse qui composent le préfixe (la partie réseau de l'adresse). Par exemple, 2001:0DB8:8086:6502::/32 est un préfixe IPv6 valide.

Le préfixe IPv6 identifie le type d'adresse IPv6. Le tableau suivant affiche les préfixes pour chaque type d'adresse IPv6.

Tableau 78 : Préfixes de type d'adresse IPv6

Type d'adresse	Préfixe binaire	Notation IPv6
Non défini	000...0 (128 bits)	::/128
Boucle avec retour	000...1 (128 bits)	::1/128
Multicast (multidiffusion)	11111111	FF00::/8
Lien local (monodiffusion)	1111111010	FE80::/10
Site local (monodiffusion)	1111111111	FEC0::/10
Global (monodiffusion)	Toutes les autres adresses.	
Anycast	Tiré de l'espace d'adressage de monodiffusion.	

Protocoles et applications

Le tableau suivant répertorie les valeurs littérales du protocole et les numéros de port; l'un ou l'autre peut être saisi dans les commandes ASA.

Tableau 79 : Valeurs littérales du protocole

Littéral	Valeur	Description
ah	51	En-tête d'authentification pour IPv6, RFC 1826.
eigrp	88	Protocole de routage de passerelle intérieure amélioré.
esp	50	Charge utile de sécurité encapsulée pour IPv6, RFC 1827.
gre	47	Encapsulation générale du routeur.
ICMP	1	Internet Control Message Protocol, RFC 792.
icmp6	58	Internet Control Message Protocol pour IPv6, RFC 2463.
igmp	2	Internet Group Management Protocol, RFC 1112.
igrp	9	Protocole de routage de passerelle intérieure.
ip	0	Protocole Internet.
ipinip	4	Encapsulation IP-en-IP.
IPsec	50	Sécurité IP. La saisie du littéral de protocole ipsec équivaut à la saisie du littéral de protocole esp.
nos	94	Système d'exploitation réseau (NetWare de Novell).
ospf	89	Protocole de routage Open Shortest Path First, RFC 1247.

Littéral	Valeur	Description
pcp	108	Protocole de compression de charge utile.
pim	103	Protocol Independent Multicast.
pptp	47	Protocole Point-to-Point Tunneling. La saisie du littéral de protocole pptp équivaut à la saisie du littéral de protocole gre.
snp	109	Protocole de réseau Sitara.
TCP	6	Protocole de commande de transmission, RFC 793.
UDP	17	Protocole de datagramme d'utilisateur, RFC 768.

Vous pouvez consulter les numéros de protocole en ligne sur le site Web de l'IANA :

http://www.iana.org/assignments/protocol-numbers

Ports TCP et UDP

Le tableau suivant répertorie les valeurs littérales et les numéros de port; l'un ou l'autre peut être saisi dans les commandes ASA. Consultez les avertissements suivants :

- L'ASA utilise le port 1521 pour SQL*Net. Il s'agit du port par défaut utilisé par Oracle pour SQL*Net. Cette valeur n'est toutefois pas conforme aux attributions de ports de l'IANA.
- L'ASA écoute RADIUS sur les ports 1645 et 1646. Si votre serveur RADIUS utilise les ports standard 1812 et 1813, vous pouvez configurer l'ASA pour qu'il écoute ces ports à l'aide des commandes **authentication-port** et **accounting-port**.
- Pour attribuer un port pour l'accès DNS, utilisez la valeur littérale **domain**, et non **dns**. Si vous utilisez **dns**, l'ASA suppose que vous souhaitez utiliser la valeur littérale **dnsix**.

Vous pouvez consulter les numéros de port en ligne sur le site Web de l'IANA :

http://www.iana.org/assignments/port-numbers

Tableau 80 : Valeurs littérales des ports

Littéral	TCP ou UDP?	Valeur	Description
aol	TCP	5190	Amérique en ligne
bgp	TCP	179	Protocole de passerelle frontière, RFC 1163
biff	UDP	512	Utilisé par le système de messagerie pour informer les utilisateurs de la réception d'un nouveau message
bootpc	UDP	68	Client du protocole de démarrage
bootps	UDP	67	Serveur du protocole de démarrage
chargen	TCP	19	Générateur de caractères

Littéral	TCP ou UDP?	Valeur	Description
cifs	TCP, UDP	3020	Protocole CIFS
citrix-ica	TCP	1494	Protocole Citrix Independent Computing Architecture (ICA)
CMD	TCP	514	Similaire à exec, sauf que cmd dispose d'une authentification automatique
ctiqbe	TCP	2748	Encodage rapide de tampon de l'interface de téléphonie de l'ordinateur
daytime	TCP	13	Heure du jour, RFC 867
supprimer	TCP, UDP	9	Supprimer
dnsix	UDP	195	Redirecteur d'audit du module de gestion des sessions DNSIX
domaine	TCP, UDP	53	DNS
echo	TCP, UDP	7	Écho
exec	TCP	512	Exécution du processus à distance
finger	TCP	79	Finger
ftp	TCP	21	Protocole de transfert de fichier (port de contrôle)
données-ftp	TCP	20	Protocole de transfert de fichier (port de données)
gopher	TCP	70	Gopher
h323	TCP	1720	Signalisation d'appel H.323
nom d'hôte	TCP	101	Serveur de noms d'hôte NIC
http	TCP, UDP	80	HTTP Internet
https	TCP	443	HTTP sur SSL
ident	TCP	113	Service d'authentification Ident
imap4	TCP	143	Protocole IMAP (Internet Message Access Protocol), version 4
irc	TCP	194	Protocole de discussion IRC (Internet Relay Chat)
isakmp	UDP	500	protocole ISAKMP (Internet Security Association and Key Management Protocol)
kerberos	TCP, UDP	750	Kerberos
klogin	TCP	543	KLOGIN

Littéral	TCP ou UDP?	Valeur	Description
kshell	TCP	544	Korn Shell
ldap	TCP	389	Protocole Lightweight Directory Access Protocol
ldaps	TCP	636	Protocole Lightweight Directory Access Protocol (SSL)
connexion	TCP	513	Connexion à distance
lotusnotes	TCP	1352	Lotus Notes IBM
lpd	TCP	515	Démon d'impression en ligne – spouleur d'impression
mobile-ip	UDP	434	Agent IP mobile
nameserver	UDP	42	Serveur de noms d'hôte
netbios-dgm	UDP	138	Service de datagrammes NetBIOS
netbios-ns	UDP	137	Service de noms NetBIOS
netbios-ssn	TCP	139	Service de sessions NetBIOS
nfs	TCP, UDP	2049	Système de fichiers réseau – Sun Microsystems
nntp	TCP	119	Protocole de transfert des informations du réseau
ntp	UDP	123	Protocole de synchronisation réseau
pcanywhere-data	TCP	5631	Données pcAnywhere
pcanywhere-status	UDP	5632	État pcAnywhere
pim-auto-rp	TCP, UDP	496	PIM (Protocole Independent Multicast), inondation de chemin inverse, mode dense
pop2	TCP	109	Protocole du bureau de poste – Version 2
pop3	TCP	110	Protocole du bureau de poste – Version 3
pptp	TCP	1723	Protocole Point-to-Point Tunneling
radius	UDP	1645	Service d'usager commuté à authentification distante
radius-acct	UDP	1646	Service d'usager commuté à authentification distante (comptabilité)
protocole RIP	UDP	520	Protocole d'information de routage
rsh	TCP	514	Shell distant
rtsp	TCP	554	Protocole de diffusion en flux continu en temps réel
secureid-udp	UDP	5510	SecureID sur UDP

Littéral	TCP ou UDP?	Valeur	Description
sip	TCP, UDP	5060	Protocole d'initiation de session (SIP)
smtp	TCP	25	Protocole de transport de messagerie simple
snmp	UDP	161	Protocole SNMP (gestion de réseau simple)
snmptrap	UDP	162	Protocole simple de gestion de réseau – Interruption
sqlnet	TCP	1521	Réseau SQL (Structured Query Language)
ssh	TCP	22	Protocole SSH (Secure Shell)
sunrpc	TCP, UDP	111	Appel de procédure à distance Sun
syslog	UDP	514	System Log (journal du système)
tacacs	TCP, UDP	49	Système de contrôle d'accès du contrôleur d'accès du terminal Plus
talk	TCP, UDP	517	Talk
telnet	TCP	23	Telnet RFC 854
tftp	UDP	69	protocole TFTP (Trivial File Transfer Protocol)
de temps	UDP	37	Durée
uucp	TCP	540	Programme de copie UNIX à UNIX
vxlan	UDP	4789	Réseau local extensible virtuel (VXLAN)
who	UDP	513	Qui
Whois	TCP	43	Qui est
www	TCP, UDP	80	Internet
xdmcp	UDP	177	Protocole de contrôle du gestionnaire d'affichage X

Ports et protocoles locaux

Le tableau suivant répertorie les protocoles, les ports TCP et les ports UDP que l'ASA peut ouvrir pour traiter le trafic destiné à l'ASA. À moins que vous activiez les fonctionnalités et les services énumérés dans ce tableau, l'ASA *n'ouvre* aucun protocole local ni port TCP ou UDP. Vous devez configurer une fonctionnalité ou un service pour que l'ASA ouvre le protocole d'écoute ou le port par défaut. Dans de nombreux cas, vous pouvez configurer des ports autres que le port par défaut lorsque vous activez une fonctionnalité ou un service.

Tableau 81 : Protocoles et ports ouverts par les fonctionnalités et services

Fonctionnalité ou service	Protocole	Numéro de port	Commentaires
DHCP (protocole de configuration dynamique des hôtes)	UDP	67,68	—
Contrôle du basculement	105	S. O.	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	S. O.	—
IGMP	2	S. O.	Protocole ouvert uniquement sur l'adresse IP de destination 224.0.0.1
ISAKMP/IKE	UDP	500	Configurable.
IPsec (ESP)	50	S. O.	—
IPsec sur UDP (NAT-T)	UDP	4500	—
IPsec sur TCP (CTCP)	TCP	—	Aucun port par défaut n'est utilisé. Vous devez spécifier le numéro de port lors de la configuration d'IPsec sur TCP.
NTP;	UDP	123	—
OSPF	89	s.o.	Protocole ouvert uniquement sur les adresses IP de destination 224.0.0.5 et 224.0.0.6
Protocole PIM	103	s.o.	Protocole ouvert uniquement sur l'adresse IP de destination 224.0.0.13
RIP	UDP	520	—
Protocole RIPv2	UDP	520	Port ouvert uniquement sur l'adresse IP de destination 224.0.0.9
SNMP	UDP	161	Configurable.
SSH	TCP	22	—
Mise à jour de l'état	8 (non sécurisé) 9 (sécurisé)	S. O.	—
Telnet	TCP	23	—
Équilibrage de la charge VPN	UDP	9023	Configurable.

Fonctionnalité ou service	Protocole	Numéro de port	Commentaires
Mandataire d'authentification de l'utilisateur individuel pour le VPN	UDP	1645, 1646	Port accessible uniquement sur le tunnel VPN.

Types ICMP

Le tableau suivant répertorie les numéros et les noms de type ICMP que vous pouvez saisir dans les commandes ASA.

Tableau 82 : Types ICMP

Numéro ICMP	Nom ICMP
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error

Numéro ICMP	Nom ICMP
32	mobile-redirect

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.