

Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire d'appareils Firepower, version 7.0

Dernière modification : 2026-07-31

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)

© 2021–2023 Cisco Systems, Inc. Tous droits réservés.

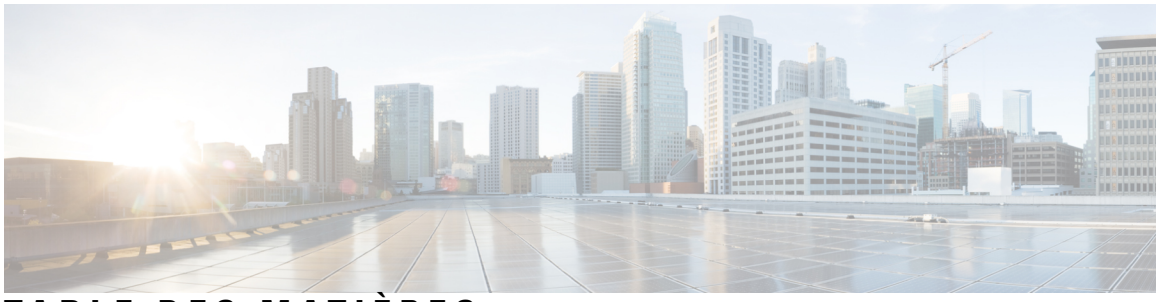


TABLE DES MATIÈRES

CHAPITRE 1

Pour commencer 1

- Ce guide est-il pour vous? 1
- Nouvelles fonctionnalités dans la version 7.0.0 de FDM/FTD 2
- Configuration par défaut 8
  - Configuration par défaut avant la configuration initiale 8
  - Configuration après la configuration initiale 11
- Connexion au système 15
  - Votre rôle d'utilisateur contrôle ce que vous pouvez voir et faire 16
  - Connectez-vous au Gestionnaire de périphériques de pare-feu. 16
  - Connexion avec l'interface de ligne de commande (CLI) 18
  - Modifier votre mot de passe 19
  - Définition des préférences de profil utilisateur 19
  - Affichage des pages dans d'autres langues que l'anglais 20
- Configuration du système 20
  - Connecter les interfaces 21
  - (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande 21
  - Compléter la configuration initiale avec l'assistant d'installation 23
  - Que faire si vous n'obtenez pas d'adresse IP pour l'interface externe 25
- Bases de la configuration 27
  - Configuration du périphérique 27
  - Configuration des politiques de sécurité 28
  - Recherche de règles ou d'objets 30
  - Déploiement des modifications 30
    - Changements de configuration qui redémarrent les moteurs d'inspection. 32
    - Modifications de configuration qui forcent un déploiement complet 33

Affichage de l'interface et de l'état de gestion 33
Affichage de l'état des tâches du système 34
Utilisation de la console d'interface de ligne de commande pour surveiller et tester la configuration 35
Utilisation conjointe de Gestionnaire de périphériques de pare-feu et de l'API REST 37
Exigences relatives aux ports de communication et à l'accès Internet 37
Ports de communication utilisés par le périphérique 38
Ressources Internet consultées par le périphérique 39

CHAPITRE 2 **Meilleures pratiques : scénarios d'utilisation pour Firewall Threat Defense 43**
Comment configurer l'appareil en FDM 43
Comment mieux comprendre le trafic de votre réseau 49
Comment bloquer les menaces 56
Comment bloquer les logiciels malveillants 61
Comment mettre en œuvre une politique d'utilisation acceptable (filtrage d'URL) 64
Comment contrôler l'utilisation des applications 69
Comment ajouter un sous-réseau 73
Comment surveiller passivement le trafic sur un réseau 78
Plus d'exemples 84

CHAPITRE 3 **Octroi de licence du système 87**
Licences Smart pour le système de pare-feu 87
Cisco Smart Software Manager 87
Communication périodique avec l'autorité de licence 88
Type de licence Smart 88
Obtention de licence pour Firewall Threat Defense Virtual 89
Lignes directrices et limites des licences de niveaux de performanceFirewall Threat Defense Virtual 90
Incidence du paramètre de contrôle des exportations sur les fonctionnalités de chiffrement 91
Incidence des licences facultatives expirées ou désactivées 91
Gestion des licences Smart 92
Enregistrement de l'appareil 93
Changer le niveau de performance Firewall Threat Defense Virtual 94
Activation ou désactivation des licences facultatives 95

Synchronisation avec Cisco Smart Software Manager 96
Désinscrire le périphérique 97
Application des licences permanentes 98
Réservation de licence permanente universelle et réservation de licence spécifique 98
Vérifier que votre compte Smart peut fournir une licence universelle 99
Passer en mode PLR et appliquer une licence universelle 99
Annuler l'enregistrement PLR 101
Annuler l'enregistrement du périphérique en mode PLR 102

PARTIE I **Surveillance du système** 103

CHAPITRE 4 **Surveillance du périphérique** 105
Activer la journalisation pour obtenir des statistiques de trafic. 105
Types d'événements 105
Journalisation des connexions configurable 106
Journalisation automatique des connexions 107
Conseils pour la journalisation des connexions 107
Envoi d'événements à un serveur Syslog externe 108
Évaluation des événements à l'aide des services en nuage Cisco 108
Tableaux de bord du trafic et du système 108
Surveillance de statistiques supplémentaires à l'aide de l'interface de ligne de commande 112
Affichage des événements 112
Configuration des vues personnalisées 114
Événements de filtrage 115
Description des champs d'événement 116

CHAPITRE 5 **Alarmes pour Cisco ISA 3000** 127
À propos des alarmes 127
Interfaces d'entrée d'alarme. 128
Interface de sortie d'alarme 128
Alarmes Syslog 129
Interruptions SNMP 129
Valeurs par défaut pour les alarmes 129
Configurer les alarmes pour l'ISA 3000 130

Configurer les contacts d'entrée d'alarme 130
Configurer les alarmes d'alimentation 132
Configurer les alarmes de température 134
Surveillance des alarmes 136
Surveillance de l'état d'alarme 136
Surveillance des messages Syslog pour des alarmes 136
Désactivation de l'alarme externe 137

PARTIE II **Objets réutilisables** 139

CHAPITRE 6 **Objets** 141
Types d'objets 141
Lignes directrices et limites relatives aux objets 144
Gestion des objets 145
Configuration des objets et des groupes de réseau. 145
Configuration des objets et groupes de ports 147
Configuration des zones de sécurité 148
Configuration des objets de filtre d'application 149
Configuration des objets et groupes d'URL. 151
Configuration des objets de géolocalisation 153
Configuration des serveurs Syslog 154
Configuration des groupes de balises de groupe de sécurité (SGT) 156

CHAPITRE 7 **Certificats** 157
Certificats 157
Chiffrement à clé publique 158
Types de certificats utilisés par fonctionnalité 158
Exemple : génération d'un certificat interne à l'aide d'OpenSSL 159
Configurer les certificats 160
Charger les certificats d'identité interne et d'autorité de certification interne 161
Génération de certificats internes autosignés et de certificats d'autorité de certification internes 163
Téléchargement des certificats de l'autorité de certification de confiance 165
Configuration des groupes de certificats CA de confiance 166

CHAPITRE 8 **Sources d'identité** 167

À propos des sources d’identité 167

Domaine d’identité Active Directory (AD) 169

Serveurs d’annuaire pris en charge 169

Limites relatives au nombre d’utilisateurs 170

Détermination du DN de base du répertoire 170

Configuration des domaines d’identité AD 171

Configuration d’une séquence de domaine AD 173

Résolution de problèmes liés aux connexions du serveur de répertoire 174

Serveurs et groupes RADIUS 176

Configurer les serveurs RADIUS 176

Configurer les groupes de serveurs RADIUS 178

Dépannage des serveurs et groupes RADIUS 179

Identity Services Engine (ISE) 180

Lignes directrices et limites pour ISE 180

Configurer Identity Services Engine (ISE) 181

Dépannage de la source d’identité ISE/ISE-PIC 183

Serveurs SAML 184

Configurer les serveurs SAML 184

Utilisateurs locaux 186

Configurer les utilisateurs locaux 187

PARTIE III **Principes de base** 189

CHAPITRE 9 **Périphériques logiques sur les appareils Firepower 4100/9300** 191

À propos des interfaces 191

Interface de gestion de châssis 191

Types d’interface 192

Interfaces FXOS par rapport aux interfaces d’application 193

Exigences et conditions préalables pour les combinaisons matérielles et logicielles de l’appareil Firepower 9300 193

Lignes directrices et limites relatives aux périphériques logiques 194

Lignes directrices et limites des interfaces 194

Lignes directrices et limites générales 194
Interfaces de configuration 195
Activer ou désactiver une interface 195
Configurer une interface physique 195
Ajouter un canal EtherChannel (canal de port) 196
Configurer un périphérique logique 197
Ajouter un FTD Standalone (Autonome) pour le FDM 197
Ajouter une paire à haute disponibilité 197
Modifier une interface sur un périphérique logique FTD 198
Se connecter à la console de l'application 201
Historique des dispositifs logiques Firepower 4100/9300 202

CHAPITRE 10 **Haute disponibilité (basculement) 203**
À propos de la haute disponibilité (basculement) 203
À propos du basculement actif/de secours 203
Rôles principal/secondaire et état actif/de secours 204
Détermination de l'unité active au démarrage 204
Événements de basculement 204
Liens de basculement et de basculement avec état 205
Lien de basculement 206
Lien de basculement dynamique 206
Interfaces pour les liens de basculement et d'état 206
Connexion des interfaces de basculement et de basculement dynamique 207
Éviter le basculement interrompu et les liaisons de données 208
Incidence du basculement dynamique sur les connexions utilisateur 209
Fonctionnalités prises en charge 209
Fonctionnalités non prises en charge 210
Modifications de configuration et actions autorisées sur une unité de secours 211
Configuration requise pour la haute accessibilité 212
Configuration matérielle requise pour la haute disponibilité 212
Configuration logicielle requise pour la haute disponibilité 212
Exigences en matière de licence pour la haute disponibilité 213
Lignes directrices pour la haute disponibilité 214
Configuration de la haute disponibilité 215

Préparer les deux unités pour la haute disponibilité 216
Configurer l'unité principale pour la haute disponibilité 218
Configurer l'unité secondaire pour la haute disponibilité 221
Configurer les critères de basculement pour la surveillance de l'intégrité 222
Configurer les critères de basculement de la surveillance de l'intégrité des unités homologues 223
Configurer les critères de basculement pour la surveillance de l'intégrité des interfaces 224
Comment le système teste l'intégrité de l'interface 226
Configurer les adresses IP et MAC de secours 227
Vérifier la High Availability Configuration (Configuration de la haute disponibilité) 228
Gérer la haute disponibilité 229
Suspendre et reprendre la haute disponibilité 230
Rupture de la haute disponibilité 232
Commutation des homologues actifs et de secours (forcer le basculement) 233
Préservation des modifications de configuration non déployées après un basculement 234
Modification des licences et de l'enregistrement en mode de haute disponibilité 235
Modification de la clé de chiffrement IPsec à haute disponibilité ou de la configuration à haute disponibilité 235
Marquer une unité défaillante comme saine 235
Mise à niveau de la haute disponibilité Firewall Threat Defense 236
Dépannage des mises à niveau de Threat Defense haute disponibilité 238
Remplacement d'une unité dans une paire à haute disponibilité 240
Surveillance de la haute disponibilité 241
Surveillance de l'état et de l'historique du basculement général 241
Surveillance de l'état pour les interfaces surveillées par la haute disponibilité 243
Surveillance des messages Syslog liés à la haute disponibilité 243
Exécution à distance des commandes CLI sur l'unité homologue 244
Dépannage de la haute disponibilité (basculement) 244
Dépannage de l'état de défaillance d'une unité 246
Dépannage des échecs de synchronisation des applications à haute disponibilité 247

CHAPITRE 11 **Interfaces** 251
À propos des interfaces Firewall Threat Defense 251
Modes d'interface 252
Interface de gestion/dépistage 253

Recommandations pour la configuration d'un réseau de gestion distinct 253
Zones de sécurité 254
Adresse IPv6 254
Fonctionnalité Auto-MDI/MDIX 255
Lignes directrices et limites des interfaces 255
Limites de la configuration de l'interface 255
Nombre maximal de sous-interfaces VLAN par modèle de périphérique 255
Configurer une interface physique 256
Configurer des groupes de ponts 261
Configurer les EtherChannels 265
À propos des EtherChannels 266
Interfaces des groupes de canaux 266
Connexion à un EtherChannel sur un autre périphérique 266
Protocole LACP (Link Aggregation Control Protocol) 268
Équilibrage de la charge 268
Adresse MAC de l'EtherChannel 268
Lignes directrices pour les EtherChannels 269
Ajouter un canal EtherChannel 271
Configurer les interfaces VLAN et les ports de commutation 276
Comprendre les ports et les interfaces de commutation 276
Préalables pour les ports de commutation 277
Lignes directrices relatives aux ports de commutation 277
Configurer une interface VLAN 278
Configurer les ports de commutation comme ports d'accès 283
Configurer les ports de commutation comme ports de ligne principale 285
Configurer Power Over Ethernet (alimentation électrique par câble Ethernet) 287
Configurer les sous-interfaces VLAN et la jonction 802.1Q 289
Configurer des interfaces passives 294
Interfaces passives 294
Limites pour les interfaces passives 295
Configurer le commutateur pour une interface matérielle FTD passive 295
Configurer le VLAN pour une interface passive FTDv 296
Configurer l'interface physique en mode passif 297
Configurer les options d'interface avancées 298

À propos des adresses MAC 298
À propos de la MTU 299
Chemin de découverte de MTU 299
MTU et fragmentation. 299
MTU et trames grand format 299
Configurer les options avancées 300
Analyser les modifications d'interface et migrer une interface 302
À propos de l'analyse et de la migration des interfaces 302
Lignes directrices et limites pour l'analyse et la migration d'interfaces 303
Analyser et migrer les interfaces 304
Configurer le contournement matériel automatique en cas de panne de courant (ISA 3000) 307
Surveillance des interfaces 310
Exemples d'interfaces 311

PARTIE IV **Routage** 313

CHAPITRE 12 **Bases de routage et routes statiques** 315
Bonnes pratiques pour le routage 315
Aperçu du routage 315
Protocoles de routage pris en charge 316
Types de route 317
La table de routage et la sélection de route 318
Mode de remplissage de la table de routage 318
Prise des décisions de transfert 320
Table de routage pour le trafic de gestion 321
Routage à chemins multiples à coûts égaux (ECMP) 322
Routes statiques 322
À propos des routages statiques et par défaut 322
Routage par défaut 322
Routes statiques 323
Routes statiques de sauvegarde et suivi de routage statique 323
Lignes directrices relatives au routage statique 324
Configuration des routes statiques 325
Configurer les objets du moniteur SLA 326

Configuration des zones de trafic ECMP 328
Surveillance du routage 330

CHAPITRE 13 Routeurs virtuels 333
À propos des routeurs virtuels et du routage et transfert virtuel (VRF) 333
Configuration des politiques pour qu'elles soient compatibles avec les routeurs virtuels 334
Routage entre routeurs virtuels 334
Nombre maximal de routeurs virtuels par modèle de périphérique 335
Lignes directrices pour les routeurs virtuels 336
Gestion des routeurs virtuels 338
Créer un routeur virtuel ou modifier les affectations d'interface 340
Configurer Static Routes (routes statiques) et Routing Processes (processus de routage) dans un routeur virtuel 341
Supprimer un routeur virtuel 341
Exemples pour les routeurs virtuels 342
Comment effectuer un routage vers un serveur distant à l'aide de routeurs virtuels 342
Fournir un accès Internet à plusieurs routeurs virtuels avec des espaces d'adresses en chevauchement 347
Surveillance des routeurs virtuels 358

CHAPITRE 14 Cartes de routage et autres objets pour le réglage du routage 359
Configurer les cartes de routage 359
Clauses d'autorisation et de refus des cartes de routage 359
Instructions de correspondance et de définition de la carte de route 360
Configurer une carte de routage 361
Configurer une liste d'accès 365
Configurer les listes de contrôle d'accès étendues. 366
Configurer les listes d'accès standard 368
Configurer des listes d'accès AS Path 369
Configurer des listes de la communauté 370
Configurer les listes de politiques 373
Configurer les listes de préfixe 375

CHAPITRE 15 Open Shortest Path First (OSPF) 379

Configurer le processus et les zones OSPFv2 379
Personnalisation des caractéristiques du processus OSPF et des zones 381
Configurer les paramètres avancés pour un processus OSPF 381
Configurer les propriétés de la zone OSPF 385
Configurer les voisins OSPF statiques 389
Configurer les adresses de résumé OSPF 390
Configurer les règles de filtre OSPF 392
Configurer la redistribution OSPF 393
Configurer les paramètres de l'interface OSPFv2 et l'authentification OSPF 395
Configurer la détection de voisin perdu OSPFv2 et les paquets Fast Hello (paramètres de l'interface OSPF) 398
Supervision OSPF 399

CHAPITRE 16 **Protocole de routage de passerelle intérieure amélioré (EIGRP)** 401
Bonnes pratiques pour l'EIGRP 401
À propos d'EIGRP 402
Machine à états finis DUAL 402
Poids métriques EIGRP 403
Mesures de coût EIGRP 403
Lignes directrices relatives à l'EIGRP 403
Configurer le processus Core EIGRP 404
Configurer le processus EIGRP pour le routage complet 404
Configurer le processus EIGRP pour le routage de talon 405
Personnaliser le processus EIGRP 408
Configurer les paramètres avancés EIGRP 408
Configurer les réseaux pour l'annonce par l'EIGRP 410
Configurer les interfaces de routage passif EIGRP 411
Configurer les voisins statiques EIGRP 412
Contrôler la diffusion de la route par défaut candidate pour l'EIGRP 413
Configurer les filtres de redistribution des routes EIGRP 414
Configurer la redistribution des routes EIGRP 415
Surveillance EIGRP 418

CHAPITRE 17 **Protocole de routage BGP** 419

À propos de BGP 419
Modifications apportées à la table de routage 419
Quand utiliser BGP 420
Sélection du chemin BGP 421
Chemins multiples BGP 421
Configurer le protocole BGP 422
Configurer les paramètres globaux BGP 423
Configurer le processus de BGP 426
Configurer les paramètres généraux BGP 428
Configurer les paramètres avancés BGP 429
Configurer les réseaux pour l'annonce par le BGP 431
Configurer l'injection de route BGP 432
Configurer les paramètres d'adresse d'association BGP 433
Configurer les paramètres de filtre de BGP pour IPv4 435
Configurer les voisins BGP 436
Configurer la redistribution du routage BGP à partir d'autres protocoles de routage 443
Supervision BGP 445

PARTIE V **Politiques de sécurité** 447

CHAPITRE 18 **Déchiffrement SSL** 449
À propos du déchiffrement SSL 449
Pourquoi mettre en œuvre le déchiffrement SSL? 449
Actions que vous pouvez appliquer au trafic chiffré 450
Déchiffrer - Resigner 450
Déchiffrer à l'aide d'une clé connue 451
Ne pas déchiffrer 452
Bloquer 452
Règles de déchiffrement SSL générées automatiquement 452
Gestion du trafic non déchiffrable 452
Exigences de licence pour le déchiffrement SSL 453
Lignes directrices pour l'utilisation du déchiffrement 453
Comment mettre en œuvre et maintenir la politique de déchiffrement SSL 454
Configuration des politiques de déchiffrement SSL 456

Activer la politique de déchiffrement SSL. 457
Configurer l'action de déchiffrement SSL par défaut 459
Configurer les règles de déchiffrement SSL 459
Critères de source/destination pour les règles de déchiffrement SSL 462
Critères d'application pour les règles de déchiffrement SSL 463
Critères d'URL pour les règles de déchiffrement SSL 464
Critères d'utilisateur pour les règles de déchiffrement SSL 465
Critères avancés pour les règles de déchiffrement SSL 466
Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement 467
Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature 469
Exemple : blocage des anciennes versions SSL/TLS du réseau 470
Surveillance et dépannage du déchiffrement SSL 472
Surveillance du déchiffrement SSL 472
Gestion des sites Web où la règle Decrypt Re-sign (Déchiffrer-Resigner) fonctionne pour un navigateur mais pas pour une application (SSL ou épinglage d'autorité de certification) 473

CHAPITRE 19 **Stratégies d'identité** 475
Aperçu de la politique d'identité 475
Établissement de l'identité de l'utilisateur par l'authentification passive 476
Établissement de l'identité de l'utilisateur par l'authentification active 476
Traiter avec des utilisateurs inconnus 476
Comment mettre en œuvre la politique d'identité 477
Configuration des politiques d'identité 478
Configurer les paramètres de la politique d'identité 479
Configurer l'action par défaut de la politique d'identité 480
Configurer les règles d'identité 481
Activation de l'authentification transparente de l'utilisateur 485
Exigences pour l'authentification transparente 486
Configuration d'Internet Explorer pour l'authentification transparente 486
Configuration de Firefox pour l'authentification transparente 487
Politiques d'identité de surveillance 488
Exemples de politiques d'identité 489

CHAPITRE 20 **Renseignements de sécurité** 491

À propos des renseignements sur la sécurité 491

Création d'exceptions aux listes de blocage 492

Catégories de flux de renseignements sur la sécurité 492

Exigences de licence pour les renseignements sur la sécurité 494

Configurer les renseignements sur la sécurité 494

Surveillance de l'intelligence de sécurité 495

Exemples pour les renseignements sur la sécurité 495

CHAPITRE 21 **Contrôle d'accès** 497

Bonnes pratiques pour les règles de contrôle d'accès 497

Aperçu du contrôle d'accès 500

Règles de contrôle d'accès et action par défaut 500

Filtrage d'applications 501

Application Control pour le trafic chiffré et déchiffré 501

Filtrage en fonction du protocole industriel commun (CIP) et des applications Modbus (ISA 3000) 501

Bonnes pratiques pour le filtrage d'applications 502

Filtrage URL 503

Filtrage des URL par catégorie et par réputation 503

Recherche de la catégorie et de la réputation d'une URL 504

Filtrage manuel des URL 504

Filtrage du trafic HTTPS 505

Comparaison du filtrage d'URL et du filtrage d'applications 506

Bonnes pratiques pour un filtrage d'URL efficace 507

Ce que l'utilisateur voit lorsque vous bloquez des sites Web 508

Filtrage des requêtes DNS 509

Lignes directrices relatives au filtrage des demandes DNS 509

Filtrage des requêtes DNS en fonction de la catégorie d'URL et de la réputation 510

Inspection des intrusions, des fichiers et des logiciels malveillants 510

Bonnes pratiques pour l'ordre des règles de contrôle d'accès 511

NAT et critères d'accès 512

Comment les autres politiques de sécurité impactent le contrôle d'accès 512

Exigences de licence pour le contrôle d'accès 512
Lignes directrices et limites pour les stratégies de contrôle d'accès 513
Configuration de la politique de contrôle d'accès 515
Configuration de l'action par défaut 516
Configuration des paramètres de la politique de contrôle d'accès 517
Configuration des règles de contrôle d'accès 517
Critères de source/de destination 519
Critères d'application 521
Critères pour les URL 523
Critères utilisateur 524
Paramètres de la politique de prévention des intrusions 526
Paramètres de la stratégie de fichier 526
Paramètres de journalisation 527
Gestion des stratégies de contrôle d'accès 529
Statistiques de contrôle d'accès dans les tableaux de bord 529
Examen du nombre de résultats pour les règles 529
Surveillance des messages Syslog pour le contrôle d'accès 530
Surveillance des stratégies de contrôle d'accès dans l'interface de ligne de commande 531
Exemples pour le contrôle d'accès 531
Comment contrôler l'accès au réseau à l'aide des balises de groupe de sécurité TrustSec 532
À propos des balises de groupe de sécurité (SGT) 532
Configurer le contrôle d'accès en fonction de la balise de groupe de sécurité (SGT) 533

CHAPITRE 22 **Stratégies de prévention des intrusions 539**
À propos des politiques d'analyse de réseau et de prévention des intrusions 539
Politiques d'analyse de réseau et de prévention des intrusions définies par le système 540
Mode d'inspection : prévention ou détection 541
Règles de prévention des intrusions et de préprocesseur 541
Attributs des règles d'intrusion 541
Ensemble de variables d'intrusion par défaut 542
Identifiants du Générateur 543
Stratégies d'analyse de réseau 545
Exigences de licence pour les politiques de prévention des intrusions 545
Application des politiques de prévention des intrusions dans les règles de contrôle d'accès 545

Commutation entre Snort 2 et Snort 3 546
Configuration de Syslog pour les événements d'intrusion 547
Gestion des politiques de prévention des intrusions Snort 3 548
Configuration d'une politique de prévention des intrusions personnalisée (Snort 3) 549
Affichage ou modification des propriétés de la politique de prévention des intrusions (Snort 3) 550
Ajout ou suppression de groupes de règles dans une politique de prévention des intrusions (Snort 3) 553
Modification des actions des règles de prévention des intrusions (Snort 3) 554
Gestion des règles de prévention des intrusions personnalisées et des groupes de règles 556
Chargement de règles de prévention des intrusions personnalisées 558
Configuration des règles de prévention des intrusions personnalisées individuelles 560
Gestion des politiques de prévention des intrusions (Snort 2) 562
Configurer le mode d'inspection d'une politique de prévention des intrusions (Snort 2) 562
Modification des actions des règles de prévention des intrusions (Snort 2) 563
Surveillance des politiques de prévention des intrusions 564
Exemples de politiques de prévention des intrusions 564

CHAPITRE 23 **Traduction d'adresses réseau (NAT)** 565
Pourquoi utiliser la NAT? 565
Principes de base de la NAT 566
Terminologie NAT 566
Types de NAT 566
NAT en mode routé 567
NAT automatique et NAT manuelle 568
NAT automatique 568
NAT manuelle 568
Comparaison de la NAT automatique et la NAT manuelle 568
Ordre des règles NAT 569
Interfaces NAT 571
Configurer le routage pour la NAT 572
Adresses sur le même réseau que l'interface mappée 572
Adresses sur un réseau unique 572
Même adresse que l'adresse réelle (NAT d'identité) 572
Directives pour la NAT 573

Directives relatives à l'interface 573
Directives pour la NAT pour IPv6 573
Bonnes pratiques pour la NAT IPv6 574
Prise en charge de la NAT pour les protocoles inspectés 574
Directives supplémentaires pour la NAT 576
Configurer la traduction d'adresses réseau (NAT) 578
Traduction d'adresses réseau dynamique 579
À propos de la NAT dynamique 579
Désavantages et avantages de la NAT dynamique 580
Configurer la NAT automatique dynamique 581
Configurer la NAT manuelle dynamique 582
PAT dynamique 584
À propos de la PAT dynamique 584
Avantages et inconvénients de la PAT dynamique 585
Configurer la PAT automatique dynamique 585
Configurer la PAT manuelle dynamique 587
NAT statique 589
À propos de la NAT statique 589
Configurer la NAT statique automatique 593
Configurer la NAT manuelle statique 595
NAT d'identité 598
Configurer la NAT automatique d'identité 599
Configurer la NAT manuelle d'identité 600
Propriétés de la règle NAT pour Firewall Threat Defense 602
Propriétés de traduction de paquets pour la NAT automatique 603
Propriétés de traduction de paquets pour la NAT manuelle 604
Propriétés NAT avancées 606
Traduction de réseaux IPv6 607
NAT64/46 : traduction d'adresses IPv6 en IPv4 607
Exemple NAT64/46 : réseau IPv6 interne avec Internet IPv4 externe 608
Exemple NAT64/46 : réseau interne IPv6 avec Internet IPv4 externe et traduction DNS 610
NAT66 : traduction d'adresses IPv6 en adresses différentes IPv6 615
Exemple NAT66, de traduction statique entre réseaux 615
Exemple de NAT66, PAT d'interface IPv6 simple 618

Surveillance de la NAT 621
Exemples relatifs à la NAT 622
Fournir l'accès à un serveur Web interne (NAT automatique statique) 622
Adresse unique pour FTP, HTTP et SMTP (NAT automatique statique avec traduction de port) 625
Traduction différente selon la destination (PAT manuelle dynamique) 631
Traduction différente selon l'adresse et le port de destination (PAT manuelle dynamique) 637
Réécriture des requêtes et des réponses DNS à l'aide de la NAT 642
Modification de la réponse DNS64 643
Modification de la réponse DNS, serveur DNS externe 649
Modification de la réponse DNS, serveur DNS sur le réseau hôte 652

PARTIE VI **Réseaux privés virtuels (VPN)** 657

CHAPITRE 24 **VPN de site à site** 659
Principes de base du VPN 659
Protocole IKE (Internet Key Exchange) 660
Dans quelle mesure une connexion VPN doit-elle être sécurisée? 661
Choix de l'algorithme de chiffrement à utiliser 661
Décider des algorithmes de hachage à utiliser 662
Choix du groupe de module Diffie-Hellman à utiliser 662
Choix de la méthode d'authentification à utiliser 663
Topologies VPN 664
Établissement de connexions VPN de site à site avec des homologues à adresse dynamique 665
Virtual Tunnel Interfaces et VPN basé sur le routage 665
Aperçu du processus de configuration des VPN basés sur le routage 666
Lignes directrices pour les interfaces de tunnel virtuel et VPN basé sur le routage 666
Gestion des VPN de site à site 667
Configuration d'une connexion VPN de site à site 668
Configuration d'une interface de tunnel virtuel 672
Autoriser le trafic via le VPN de site à site 673
Configuration de la politique IKE globale 674
Configuration des politiques IKEv1 675
Configuration des politiques IKEv2 677
Configuration des propositions IPsec 679

Configuration des propositions IPsec pour IKEv1 679
Configuration des propositions IPsec pour IKEv2 680
Vérification des connexions VPN de site à site 681
Supervision du VPN de site à site 684
Exemples de VPN de site à site 685
Exemption du trafic VPN de site à site de la NAT 685
Comment fournir un accès Internet sur l'interface externe pour les utilisateurs d'un VPN site à site externe (hairpinning) 691
Sécuriser le trafic de réseaux dans plusieurs routeurs virtuels sur un VPN de site à site 698

CHAPITRE 25 **VPN d'accès à distance 703**
Aperçu du VPN d'accès à distance 703
Nombre maximal de sessions VPN simultanées par modèle de périphérique 703
Téléchargement du logiciel client AnyConnect 704
Comment les utilisateurs peuvent installer le logiciel client AnyConnect 705
Contrôle des autorisations et des attributs des utilisateurs à l'aide de RADIUS et des stratégies de groupe 705
Attributs envoyés au serveur RADIUS 706
Attributs reçus du serveur RADIUS 707
Authentification à deux facteurs 708
Authentification à deux facteurs RSA 708
Authentification à deux facteurs Duo au moyen de RADIUS 708
Authentification à deux facteurs Duo avec LDAP 709
Exigences de licence pour le VPN d'accès à distance 710
Consignes et limites pour le VPN d'accès à distance 710
Configuration du VPN d'accès à distance 711
Configurer et charger les profils client AnyConnect 713
Autoriser le trafic par le VPN d'accès à distance 715
Vérifier la configuration VPN d'accès à distance 716
Gestion de la configuration VPN d'accès à distance 718
Configurer un profil de connexion VPN d'accès à distance 718
Configurer AAA pour un profil de connexion 722
Configurer l'authentification par certificat pour un profil de connexion 725
Configurer l'adressage client pour le VPN d'accès à distance 726

Configurer les politiques de groupe pour le VPN d'accès à distance 726
Attributs généraux 727
Attributs des paramètres de session 728
Attributs d'attribution d'adresse 729
Attributs de tunnellisation fractionnée 729
Attributs client AnyConnect 730
Attributs des filtres de trafic 732
Attributs de mandataire de navigateur Windows 732
Surveillance du VPN d'accès à distance 733
Dépannage des VPN d'accès à distance 733
Dépannage des problèmes de connexion SSL 733
Dépannage des problèmes de téléchargement et d'installation client AnyConnect 734
Dépannage des problèmes de connexionclient AnyConnect 734
Dépannage des problèmes de flux de trafic du VPN d'accès à distance 735
Exemples d'utilisation du VPN d'accès à distance 736
Comment mettre en œuvre la modification d'autorisation RADIUS 736
Flux système pour la modification d'autorisation 736
Configurer Change of Authorization (modification d'autorisation) sur le périphérique Firewall Threat Defense 738
Configurer la modification d'autorisation dans ISE 741
Comment configurer l'authentification à deux facteurs à l'aide de Duo LDAP 745
Flux système pour l'authentification secondaire Duo LDAP 745
Configurer l'authentification secondaire Duo LDAP 746
Comment fournir un accès Internet sur l'interface externe pour les utilisateurs du VPN d'accès à distance (Hair Pinning) 752
Comment utiliser un serveur de répertoire sur un réseau externe avec le VPN d'accès à distance 757
Comment contrôler l'accès VPN RA par groupe 772
Comment autoriser l'accès au VPN d'accès à distance aux réseaux internes dans différents routeurs virtuels. 775
Comment personnaliser l'icône et le logo client AnyConnect 779

PARTIE VII **Administration système** 783

CHAPITRE 26 **Paramètres système** 785

Configurer l'accès de gestion 785
Configuration de la liste d'accès de gestion 786
Configuration du port HTTPS pour l’accès de gestion sur les interfaces de données 788
Configuration du certificat du serveur Web Firewall Threat Defense 788
Configurer les paramètres de journalisation du système 789
Niveaux de gravité 790
Configurer la journalisation vers un serveur Syslog distant 790
Configuration de la journalisation dans le tampon interne 792
Configuration de la journalisation sur la console 793
Configurer Event List Filters (Filtres de liste d’événements) 793
Configuration du serveur DHCP 795
Configurer le DNS 797
Configuration des groupes DNS 797
Configuration DNS pour les données et le trafic de gestion 798
Dépannage des problèmes généraux de DNS 800
Configuration de l'interface de gestion 802
Configurer le nom d’hôte du périphérique. 804
Protocole de temps réseau (NTP) 804
Configuration du protocole Precision Time Protocol (PTP) (ISA 3000) 805
Configuration du serveur mandataire HTTP pour les connexions de gestion 808
Configuration de Cisco Cloud Services 809
Activation ou désactivation Contrôle de Security Cloud (Legacy Device Manager Mode (mode de gestionnaire d’appareil existant)) 810
Connexion à Cisco Success Network 811
Envoi d'événements à Cisco Cloud 812
Se désinscrire de Cisco Cloud services 813
Activation ou désactivation de l’analyse Web 814
Configuration des préférences de filtrage Cloud 814
Configuration des paramètres de chiffrement TLS/SSL 815
Configurer les objets de chiffrement TLS/SSL 816

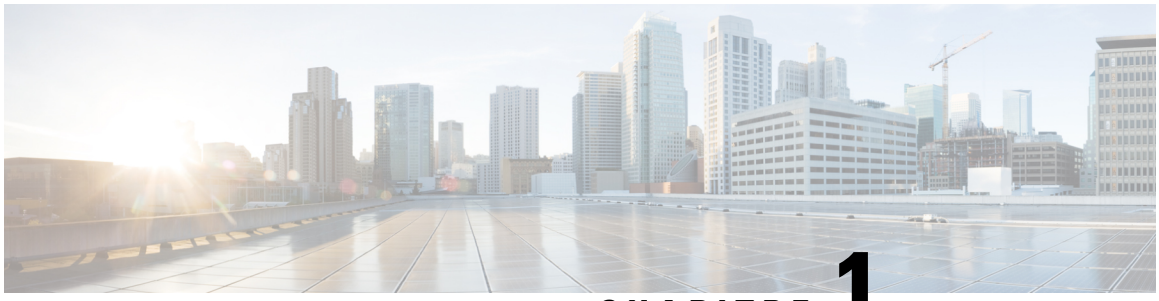
CHAPITRE 27 **Gestion du système 819**
Installation des mises à jour logicielles 819
Mise à jour des bases de données système et des flux 819

Aperçu des mises à jour de la base de données du système et des flux 819
Mise à jour des bases de données du système. 821
Mise à jour des flux de renseignements de sécurité 823
Mise à niveau Firewall Threat Defense 824
Exécution d'une vérification de l'état de préparation aux mises à niveau 825
Surveillance des mises à niveau de Firewall Threat Defense 826
Annulation ou nouvelle tentative des Firewall Threat Defense mises à niveau 827
Rétablissement Firewall Threat Defense en cours... 827
Dépannage des mises à niveau de la protection contre les menaces 828
Recréation d'image du périphérique 830
Sauvegarde et restauration du système 830
Sauvegarder le système immédiatement 831
Sauvegarder le système à une heure planifiée 832
Configuration d'une planification de sauvegarde récurrente 833
Restauration d'une sauvegarde 834
Gestion des fichiers de sauvegarde 835
Audit et gestion du changement 836
Événements d'audit 836
Visualisation et analyse du journal d'audit 838
Filtrage du journal d'audit 839
Examen du déploiement et de l'historique des modifications d'entité 841
Annuler toutes les modifications en attente 842
Exporter la configuration du périphérique. 843
Gestion du Gestionnaire de périphériques de pare-feu et accès des utilisateurs Firewall Threat Defense 843
Configuration de l'autorisation externe (AAA) pour les utilisateurs HTTPS Gestionnaire de périphériques de pare-feu 844
Configuration de l'autorisation externe (AAA) pour les utilisateurs de l'interface de commande (SSH) Firewall Threat Defense 846
Gérer les sessions des utilisateurs Gestionnaire de périphériques de pare-feu 847
Activation de l'accès Gestionnaire de périphériques de pare-feu sur une unité de secours à haute disponibilité pour les utilisateurs externes 848
Création de comptes d'utilisateur locaux pour l'interface de ligne de commande de Firewall Threat Defense 848
Redémarrage ou arrêt du système 850

Dépannage du système 851
Envoi de requêtes ping pour tester la connectivité 851
Suivi des routes vers les hôtes 854
Faire apparaître le périphérique sur les Traceroutes 855
Dépannage du protocole NTP 857
Dépannage du DNS pour l'interface de gestion 858
Analyse de l'utilisation du processeur et de la mémoire 861
Afficher les journaux des événements 862
Création d'un fichier de dépannage 863
Basculement entre la gestion locale et la gestion à distance 864
Tâches de gestion du matériel 867
Remplacement d'un périphérique ISA 3000 867

ANNEXE A **Configuration avancée** 869
À propos de Smart CLI et de FlexConfig 869
Utilisation conseillée pour Smart CLI et FlexConfig 870
Commandes CLI dans les objets Smart CLI et les objets FlexConfig 870
Incidence des mises à niveau logicielles sur la politique FlexConfig 871
Déterminer la version du logiciel du périphérique ASA et la configuration actuelle de la CLI 871
Commandes CLI interdites 872
Modèles Smart CLI 878
Lignes directrices et limites de Smart CLI et FlexConfig 879
Configuration des objets Smart CLI 880
Configurer la politique FlexConfig 881
Configurer les objets FlexConfig 883
Création de variables dans un objet FlexConfig 885
Référence aux variables FlexConfig et récupération de leurs valeurs 886
Références de variable : {{variable}} ou {{{variable}}} 886
Sections {{#key}} {{/key}} et sections inverses {{^key}} {{/key}} 889
Référence aux objets Smart CLI dans un objet FlexConfig 891
Configuration des objets de clé secrète 892
Dépannage de la politique FlexConfig 893
Exemples de FlexConfig 894
Comment activer et désactiver les inspections globales par défaut 895

Comment annuler vos modifications FlexConfig 900
Comment activer les inspections pour les classes de trafic uniques 902



CHAPITRE 1

Pour commencer

Les rubriques suivantes expliquent comment commencer la configuration de Cisco Firepower Threat Defense (FTD) .

- Ce guide est-il pour vous?, à la page 1
- Nouvelles fonctionnalités dans la version 7.0.0 de FDM/FTD, à la page 2
- Configuration par défaut, à la page 8
- Connexion au système, à la page 15
- Configuration du système, à la page 20
- Bases de la configuration, à la page 27
- Exigences relatives aux ports de communication et à l'accès Internet, à la page 37

Ce guide est-il pour vous?

Ce guide explique comment configurer Firepower Threat Defense à l'aide de l'interface de configuration Web Cisco Firepower Device Manager (FDM) incluse sur les appareils Firepower Threat Defense.

Le FDM vous permet de configurer les fonctionnalités de base du logiciel, les plus couramment utilisées pour les réseaux de petite ou moyenne taille. Il est spécialement conçu pour les réseaux qui comprennent un seul dispositif ou quelques-uns, pour lesquels vous ne souhaitez pas utiliser un gestionnaire de dispositifs multiples de grande puissance qui permet de contrôler un grand réseau contenant de nombreux dispositifs Firepower Threat Defense.

Si vous gérez un grand nombre d'appareils, ou si vous voulez utiliser les fonctions et configurations plus complexes que permet Firepower Threat Defense, utilisez Cisco Firepower Management Center (FMC) pour configurer vos périphériques au lieu du FDM intégré.

Vous pouvez utiliser FDM sur les périphériques suivants.

Tableau 1 : Modèles compatibles FDM

Modèle du périphérique	Version minimale du logiciel FTD
Firepower 1010, 1120, 1140	6.4
Firepower 1150	6.5
Firepower 2110, 2120, 2130, 2140	6.2.1
Firepower 4110, 4120, 4140, 4150	6.5

Modèle du périphérique	Version minimale du logiciel FTD
Firepower 4112	6.6
Firepower 9300	6.5
FTDv (FTDv) pour VMware	6.2.2
FTDv pour la machine virtuelle basée sur le noyau (KVM)	6.2.3
FTDv pour le nuage Microsoft Azure	6.5
FTDv pour le nuage Amazon Web Services (AWS)	6.6
ASA 5508-X, 5516-X	6.1
ISA 3000 (Cisco 3000 Series Industrial Security Appliances)	6.2.3

Nouvelles fonctionnalités dans la version 7.0.0 de FDM/FTD

Date de sortie : 26 mai 2021

Le tableau suivant répertorie les nouvelles fonctions disponibles dans Firepower Threat Defense 7.0.0 lorsqu'elles sont configurées à l'aide de FDM.

Fonctionnalités	Description
Caractéristiques de la plateforme	
FTDv pour HyperFlex et Nutanix.	Nous avons introduit FTDv pour Cisco HyperFlex et Nutanix Enterprise Cloud.
FTDv pour VMware vSphere/VMware ESXi 7.0.	Vous pouvez maintenant déployer FTDv sur VMware vSphere/VMware ESXi 7.0. Notez que la version 7.0 supprime également la prise en charge de VMware 6.0. Mettez à niveau l'environnement d'hébergement à une version prise en charge avant de mettre à niveau le FTD.
Nouveau mot de passe par défaut pour FTDv sur AWS.	Sur AWS, le mot de passe administrateur par défaut pour le FTDv est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (Détails avancés)** > **User Data (données utilisateur)**) lors du déploiement initial.

Fonctionnalités	Description
Prise en charge d'ISA 3000 pour l'arrêt.	Dans les versions 7.0.2 et ultérieures, vous pouvez éteindre l'ISA 3000; auparavant, vous pouviez uniquement redémarrer le périphérique. Dans les versions 7.0.5 et ultérieures, lorsque vous éteignez l'ISA 3000, le voyant DEL système s'éteint. Attendez au moins 10 secondes avant de couper l'alimentation du périphérique. Restrictions de version : la version 7.1 rend temporairement obsolète la prise en charge de cette fonctionnalité. Le soutien est de retour dans la version 7.2.
Fonctionnalités de pare-feu et IPS	
Nouvelle section 0 pour les règles NAT définies par le système.	Une nouvelle section 0 a été ajoutée au tableau de règles NAT. Cette section est destinée exclusivement à l'utilisation du système. Toutes les règles NAT dont le système a besoin pour le fonctionnement normal sont ajoutées à cette section, et ces règles ont priorité sur toutes les règles que vous créez. Auparavant, les règles définies par le système étaient ajoutées à la section 1, et les règles définies par l'utilisateur pouvaient interférer avec le bon fonctionnement du système. Vous ne pouvez pas ajouter, modifier ou supprimer les règles de la section 0, mais vous les verrez dans la sortie de la commande **show nat detail**.
Règles de prévention des intrusions personnalisées pour Snort 3.	Vous pouvez utiliser des outils hors ligne pour créer des règles de prévention des intrusions personnalisées à utiliser avec Snort 3 et les téléverser dans une politique de prévention des intrusions. Vous pouvez organiser les règles personnalisées dans vos propres groupes de règles personnalisées pour faciliter leur mise à jour au besoin. Vous pouvez également créer les règles directement dans FDM, mais les règles ont le même format que les règles téléversées. FDM ne vous guide pas dans la création des règles. Vous pouvez dupliquer des règles existantes, y compris des règles définies par le système, comme base pour une nouvelle règle de prévention des intrusions. Nous avons ajouté la prise en charge des groupes et des règles personnalisés à la page **Policies (Politiques)** > **Intrusion**, lorsque vous modifiez une politique de prévention des intrusions.
Nouvelles fonctionnalités de Snort 3 pour les systèmes gérés par FDM.	Vous pouvez désormais configurer les fonctionnalités supplémentaires suivantes lors de l'utilisation de Snort 3 comme moteur d'inspection sur un système géré par FDM : • Règles des politiques de contrôle d'accès basées sur le temps (API FTD seulement.) • Routeurs virtuels multiples • Le déchiffrement des connexions TLS 1.1 ou version inférieure à l'aide de la politique de déchiffrement SSL. • Le déchiffrement des protocoles suivants à l'aide de la politique de déchiffrement SSL : FTPS, SMTPS, IMAPS, POP3S.

Fonctionnalités	Description
Filtrage des requêtes DNS en fonction de la catégorie d'URL et de la réputation.	Vous pouvez appliquer vos règles de catégorie et de réputation de filtrage d'URL aux demandes de consultation DNS. Si le nom de domaine complet (FQDN) dans la demande de recherche dispose d'une catégorie et d'une réputation que vous bloquez, le système bloque la réponse DNS. Étant donné que l'utilisateur ne reçoit pas de résolution DNS, l'utilisateur ne peut pas établir la connexion. Utilisez cette option pour appliquer un filtrage de catégorie et de réputation d'URL au trafic non Web. Vous devez avoir une licence de filtrage d'URL pour utiliser cette fonctionnalité. Nous avons ajouté l'option d' **application de la réputation sur le trafic DNS** aux paramètres de politique de contrôle d'accès.
VDB plus petite pour les périphériques à mémoire inférieure avec Snort 2.	**Incidence de la mise à niveau. L'identification de l'application sur les périphériques à mémoire limitée est affectée.** Pour les périphériques des versions 7.0.6 et ultérieures avec Snort 2, pour VDB 363+, le système installe maintenant une VDB de taille plus faible (également appelée *VDB lite*) sur les périphériques de mémoire limitée exécutant Snort 2. Cette plus petite VDB contient les mêmes applications, mais moins de schémas de détection. Les périphériques utilisant la plus petite VDB peuvent ne pas identifier certaines applications par rapport aux périphériques utilisant la VDB complète. Périphériques de mémoire inférieure : ASA-5508-X, ASA-5516-X Restrictions de version: la VDB de taille plus faible n'est pas prise en charge par toutes les versions. Si vous effectuez une mise à niveau à partir d'une version prise en charge vers une version non prise en charge, vous ne pouvez pas installer VDB 363+ sur les périphériques de mémoire inférieure exécutant Snort 2. Pour obtenir la liste des versions concernées, consultez CSCwd88641.
Fonctionnalités du VPN	
Paramètres de chiffrement SSL FDM pour le VPN d'accès à distance.	Vous pouvez définir les versions TLS et les chiffrements à utiliser pour les connexions de VPN d'accès à distance dans FDM. Auparavant, vous deviez utiliser l'API Firepower Threat Defense pour configurer les paramètres SSL. Nous avons ajouté les pages suivantes :**Objets** > **Chiffrements SSL**; **Périphérique** > **Paramètres système** > **Paramètres SSL**.
Prise en charge de Diffie-Hellman, groupe 31.	Vous pouvez désormais utiliser le groupe 31 de Diffie-Hellman (DH) dans les propositions et les politiques IKEv2.
Le nombre maximal d'interfaces de tunnel virtuel sur le périphérique est de 1024.	Le nombre maximal d'interfaces de tunnel virtuel (VTI) que vous pouvez créer est de 1024. Dans les versions précédentes, le maximum était de 100 par interface source.

Fonctionnalités	Description
Paramètres de durée de vie IPsec pour les associations de sécurité VPN de site à site.	Vous pouvez modifier les paramètres par défaut relatifs à la durée de conservation d'une association de sécurité avant de devoir être renégociée. Nous avons ajouté les options de **durée de vie** et **d'étendue de vie** à l'assistant VPN de site à site.
Fonctionnalités de routage	
Prise en charge des routeurs virtuels pour ISA 3000.	Vous pouvez configurer jusqu'à 10 routeurs virtuels sur un périphérique ISA 3000.
Routage à chemins multiples à coûts égaux (ECMP).	Vous pouvez configurer des zones de trafic ECMP pour contenir plusieurs interfaces, ce qui permet au trafic d'une connexion existante de sortir ou d'entrer dans le périphérique Firepower Threat Defense sur n'importe quelle interface de la zone. Cette fonctionnalité permet le routage à chemins multiples à coûts égaux (ECMP) sur le périphérique Firepower Threat Defense, ainsi qu'à équilibrer la charge externe du trafic vers le périphérique Firepower Threat Defense sur plusieurs interfaces. Les zones de trafic ECMP sont utilisées uniquement pour le routage. Elles ne correspondent pas aux zones de sécurité. Nous avons ajouté l'onglet **ECMP Traffic Zones** (Zones de trafic ECMP) aux pages de routage. Dans l'API Firepower Threat Defense, nous avons ajouté les ressources ECMPZones.
Fonctionnalités de l'interface	
Nouvelle adresse IP interne par défaut.	L'adresse IP par défaut de l'interface interne est remplacée par **192.168.95.1** au lieu de 192.168.1.1 pour éviter un conflit d'adresses IP lorsqu'une adresse sur 192.168.1.0/24 est attribuée à l'interface externe à l'aide de DHCP.
La configuration automatique IPv6 de l'adresse IP externe par défaut est maintenant activée; nouveau serveur DNS IPv6 par défaut pour la gestion.	La configuration par défaut sur l'interface externe comprend désormais la configuration automatique IPv6, en plus du client DHCP IPv4. Les serveurs DNS de gestion par défaut comprennent désormais un serveur IPv6 : 2620:119:35::35.
Prise en charge d'EtherChannel pour ISA 3000.	Vous pouvez maintenant utiliser FDM pour configurer les EtherChannels sur l'ISA 3000. Écrans nouveaux ou modifiés : **Devices (Périphériques)** > **interfaces** > **EtherChannels**
Caractéristiques de la licence	

Fonctionnalités	Description
Licence progressive en fonction de la performance pour FTDv.	Le FTDv prend désormais en charge les licences Smart par niveau de performance en fonction des exigences de débit et des limites de session de VPN d'accès à distance. Lorsque le FTDv est concédé avec l'une des licences de performance disponibles, deux choses se produisent. Tout d'abord, un limiteur de débit est installé qui limite le débit du périphérique à un niveau spécifié. Ensuite, le nombre de sessions VPN est plafonné au niveau spécifié par la licence.
Fonctions d'administration et de dépannage	
Configuration du relais DHCP à l'aide de l'API Firepower Threat Defense.	**Incidence sur la mise à niveau. Peut empêcher le déploiement après la mise à niveau.** Vous pouvez utiliser l'API Firepower Threat Defense pour configurer le relais DHCP. L'utilisation du relais DHCP sur une interface vous permet de diriger les requêtes DHCP vers un serveur DHCP accessible par l'autre interface. Vous pouvez configurer le relais DHCP sur les interfaces physiques, les sous-interfaces, les interfaces VLAN et les canaux EtherChannels. Vous ne pouvez pas configurer le relais DHCP si vous configurez un serveur DHCP sur n'importe quelle interface. Notez que si vous avez utilisé FlexConfig dans les versions précédentes pour configurer le relais DHCP (la commande **dhcprelay**, vous devez refaire la configuration à l'aide de l'API et supprimer l'objet FlexConfig après la mise à niveau. Nous avons ajouté le modèle suivant à l'API Firepower Threat Defense : dhcprelayservices
Traitement de démarrage initial plus rapide et connexion anticipée à FDM.	Le processus de démarrage initial d'un système géré par FDMa été amélioré pour le rendre plus rapide. Ainsi, vous n'avez pas besoin d'attenter aussi longtemps après le démarrage du périphérique pour vous connecter à FDM. En outre, vous pouvez désormais vous connecter pendant le démarrage. Si le démarrage n'est pas terminé, vous verrez des informations d'état sur le processus afin que vous sachiez ce qui se passe sur le périphérique.
Amélioration de l'utilisation et des performances du processeur pour les connexions plusieurs à un et un à plusieurs.	Le système ne crée plus d'objets hôtes locaux et les verrouille lors de la création de connexions, sauf pour les connexions qui impliquent une NAT/PAT dynamique, l'analyse de la détection des menaces et des statistiques de l'hôte. Cela améliore les performances et l'utilisation de la CPU dans les situations où de nombreuses connexions sont dirigées vers le même serveur (comme un équilibreur de charge ou un serveur Web), ou un point terminal établit des connexions à de nombreux hôtes distants. Nous avons modifié les commandes suivantes : **clear local-host** (obsolète), **show local-host**

Fonctionnalités	Description
Vérification de l'état de préparation à la mise à niveau pour les périphériques gérés par FDM.	Vous pouvez exécuter une vérification de l'état de préparation à la mise à niveau sur un ensemble de mise à niveau Firepower Threat Defense téléchargé avant de tenter de l'installer. La vérification de l'état de préparation vérifie que la mise à niveau est valide pour le système et que le système répond aux autres exigences nécessaires à l'installation du paquet. L'exécution d'une vérification de l'état de préparation à la mise à niveau vous permet d'éviter les échecs d'installation. Un lien pour exécuter la vérification de l'état de préparation à la mise à niveau a été ajouté à la section **System Upgrade (Mise à niveau du système)** de la page **Device (Périphérique)** > **Updates (Mises à jour)**.
Mettre automatiquement à jour les ensembles d'autorités de certification.	**Incidence sur la mise à niveau. Le système se connecte à Cisco dans le cadre d'une nouveauté.** L'offre groupée de l'autorité de certification locale contient des certificats pour accéder à plusieurs services Cisco. Le système interroge désormais automatiquement Cisco pour obtenir de nouveaux certificats d'autorité de certification à une heure quotidienne définie par le système. Auparavant, vous deviez mettre à niveau le logiciel pour mettre à jour les certificats d'autorité de certification. Vous pouvez utiliser l'interface de ligne de commande pour désactiver cette fonctionnalité. Nouvelles ressources : https://cisco.com/security/pki/ Commandes CLI nouvelles ou modifiées : **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Restrictions de version : nécessite la version 7.0.5, 7.1.0.3 ou 7.2.4. Non pris en charge avec les versions 7.0.0 à 7.0.4, 7.1.0 à 7.1.0.2 ou 7.2.0 à 7.2.3. Voir : *Référence des commandes de défense contre les menaces de Cisco Secure Firewall*

Fonctionnalités	Description
Exiger l'attribut Message-Authenticator dans toutes les réponses RADIUS.	**Incidence sur la mise à niveau. Après la mise à niveau, lancez l'activation pour les serveurs existants.** Vous pouvez désormais exiger l'attribut Message-Authenticator dans toutes les réponses RADIUS, en vous assurant que la passerelle VPN de défense contre les menaces vérifie de manière sécurisée chaque réponse du serveur RADIUS, qu'il s'agisse d'un VPN d'accès à distance ou de l'accès au périphérique lui-même. L'option **Require Message-Authenticator for all RADIUS Responses** (exiger l'authentificateur Message-Authenticator pour toutes les réponses envoyées par RADIUS) est activée par défaut pour les nouveaux serveurs RADIUS. Nous vous recommandons également de l'activer pour les serveurs existants. Sa désactivation peut exposer les pare-feu à des attaques potentielles. Nouvelles commandes CLI : **message-authenticator-required** Restrictions de version : nécessite la version 7.0.7/ 7.7.0 (ou version ultérieure).
API REST de FTD version 6.1 (v6).	L'API REST Firepower Threat Defense pour la version logicielle 7.0 est la version 6.1. Vous pouvez utiliser la v6 dans les URL d'API ou, de préférence, utiliser /latest/ pour signifier que vous utilisez la version d'API la plus récente prise en charge sur le périphérique. Notez que l'élément de chemin de version d'URL pour la version 6.1 est le même que pour la version 6.0 : v6. Veuillez réévaluer tous les appels existants, car des modifications peuvent avoir été apportées aux modèles de ressources que vous utilisez. Pour ouvrir l'API Explorer et consulter les ressources, connectez-vous à FDM, cliquez sur le bouton Plus d'options (⋮) et choisissez **API Explorer**.

Configuration par défaut

La configuration par défaut de votre périphérique dépend de la réussite de la configuration initiale.

Configuration par défaut avant la configuration initiale

Avant que vous ne configuriez initialement Firepower Threat Defensel'appareil à l'aide du gestionnaire local (FDM), l'appareil comprend la configuration par défaut suivante.

Pour de nombreux modèles, cette configuration suppose que vous ouvrez le gestionnaire d'appareils au moyen de l'interface interne, généralement en branchant votre ordinateur directement sur l'interface, et que vous utilisez le serveur DHCP défini sur l'interface interne pour fournir une adresse IP à votre ordinateur. Sinon, vous pouvez relier votre ordinateur à l'interface de gestion et utiliser DHCP pour obtenir une adresse. Cependant, certains modèles ont des configurations et des exigences de gestion par défaut différentes. Reportez-vous au tableau ci-dessous pour en savoir plus.

Remarque Vous pouvez préconfigurer un grand nombre de ces paramètres à l'aide de la configuration de l'interface de ligne de commande ((Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 21) avant d'effectuer la configuration à l'aide de l'assistant.

Paramètres de configuration par défaut

Paramètres	Par défaut	Peut-on le modifier lors de la configuration initiale ?
Mot de passe de l'utilisateur admin.	Admin123 Firepower 4100/9300 : Définissez le mot de passe lorsque vous déployez le périphérique logique. AWS : La valeur par défaut est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details** > **User Data**) lors du déploiement initial.	Oui. Vous devez changer le mot de passe par défaut.
Adresse IP de gestion.	Obtenue par DHCP. FTDv192.168.45.45 Firepower 4100/9300 : Définissez l'adresse IP de gestion lorsque vous déployez le périphérique logique.	Non. Pour Firepower 4100/9300 : Oui.
Passerelle de gestion.	Les interfaces de données sur l'appareil. Généralement, l'interface externe devient la voie vers Internet. Cette passerelle fonctionne uniquement pour le trafic depuis l'appareil. Si le périphérique reçoit une passerelle par défaut du serveur DHCP, cette passerelle est utilisée. Firepower 4100/9300 : Définissez l'adresse IP de passerelle lorsque vous déployez le périphérique logique. ISA 3000 : 192.168.45.1. FTDv : 192.168.45.1	Non. Pour Firepower 4100/9300 : Oui.

Paramètres	Par défaut	Peut-on le modifier lors de la configuration initiale ?
Serveurs DNS pour l'interface de gestion.	Les serveurs DNS publics OpenDNS, IPv4 : 208.67.220.220 et 208.67.222.222; IPv6 : 2620:119:35::35. Les serveurs DNS obtenus à partir du protocole DHCP ne sont jamais utilisés. Firepower 4100/9300 : Définissez les serveurs DNS lorsque vous déployez le périphérique logique.	Oui
Adresse IP de l'interface interne.	192.168.95.1/24 Firepower 4100/9300 : Les interfaces de données ne sont pas préconfigurées. ISA 3000 : l'adresse IP BVI1 n'est pas préconfigurée. BVI1 comprend toutes les interfaces internes et externes. FTDv : 192.168.45.1/24	Non.
Serveur DHCP pour les clients internes.	Fonctionne sur l'interface interne avec l'ensemble d'adresses 192.168.95.5 à 192.168.95.254. Firepower 4100/9300 : Aucun serveur DHCP activé. ISA 3000 : Aucun serveur DHCP activé. FTDv : L'ensemble d'adresses sur l'interface interne est 192.168.45.46 à 192.168.45.254.	Non.
Configuration automatique DHCP pour les clients internes. (La configuration automatique fournit aux clients des adresses pour les serveurs WINS et DNS.)	Activé sur l'interface externe.	Oui, mais indirectement. Si vous configurez une adresse IPv4 statique pour l'interface externe, la configuration automatique du serveur DHCP est désactivée.
Adresse IP de l'interface externe.	IPv4 : Obtenu par DHCP auprès d'un fournisseur de services Internet (ISP) ou d'un routeur en amont. IPv6 : Configuration automatique. Firepower 4100/9300 : Les interfaces de données ne sont pas préconfigurées. ISA 3000 : l'adresse IP BVI1 n'est pas préconfigurée. BVI1 comprend toutes les interfaces internes et externes.	Oui.

Interfaces par défaut par modèle de périphérique

Vous ne pouvez pas sélectionner différentes interfaces internes et externes lors de la configuration initiale. Pour modifier les affectations d'interface après la configuration, modifiez les paramètres d'interface et de DHCP. Vous devez supprimer une interface du groupe de ponts avant de pouvoir la configurer en tant qu'interface non commutée.

FTDpériphérique	Interface externe	Interface interne
ASA 5508-X ASA 5516-X	GigabitEthernet 1/1	GigabitEthernet 1/2
Firepower 1010	Ethernet 1/1	VLAN1, qui comprend tous les autres ports de commutation, à l'exception de l'interface externe, qui est une interface physique de pare-feu.
Firepower 1120, 1140, 1150	Ethernet 1/1	Ethernet 1/2
Firepower de la série 2100	Ethernet 1/1	Ethernet 1/2
Firepower 4100	Les interfaces de données ne sont pas préconfigurées.	Les interfaces de données ne sont pas préconfigurées.
Firepower 9300	Les interfaces de données ne sont pas préconfigurées.	Les interfaces de données ne sont pas préconfigurées.
FTDv	GigabitEthernet 0/0	GigabitEthernet 0/1
ISA 3000	GigabitEthernet 1/1 et GigabitEthernet 1/3 GigabitEthernet 1/1 (externe1) et 1/2 (interne1) et GigabitEthernet 1/3 (externe2) et 1/4 (interne2) (modèles sans fibre uniquement) sont configurés comme paires de contournement matériel. Toutes les interfaces internes et externes font partie de BVI1.	GigabitEthernet 1/2 et GigabitEthernet 1/4

Configuration après la configuration initiale

Après avoir terminé l'assistant de configuration, la configuration du périphérique inclura les paramètres suivants. Le tableau indique si un paramètre particulier est quelque chose que vous avez choisi explicitement ou s'il a été défini pour vous en fonction de vos autres sélections. Validez toutes les configurations « impliquées » et modifiez-les si elles ne répondent pas à vos besoins.



Remarque Le Firepower 4100/9300 et ISA 3000 ne prennent pas en charge l'assistant de configuration. Pour Firepower 4100/9300, toute la configuration initiale est définie lorsque vous déployez le périphérique logique à partir du châssis. Pour l'ISA 3000, une configuration spéciale par défaut est appliquée avant l'expédition.

Paramètres	Configuration	Configuration explicite, implicite ou par défaut
Mot de passe de l'utilisateur admin.	Quoi que vous ayez saisi.	Explicite.
Adresse IP de gestion.	Obtenue par DHCP. FTDv: 192.168.45.45 Firepower 4100/9300: vous avez défini l'adresse IP de gestion lorsque vous avez déployé le dispositif logique.	Situations de défaillance.
Passerelle de gestion.	Les interfaces de données sur l'appareil. Généralement, l'interface externe devient la voie vers Internet. Cette passerelle fonctionne uniquement pour le trafic provenant du périphérique. Si le périphérique reçoit une passerelle par défaut du serveur DHCP, cette passerelle est utilisée. Firepower 4100/9300: l'adresse IP de passerelle que vous avez définie lorsque vous avez déployé le périphérique logique. ISA 3000: 192.168.45.1 FTDv : 192.168.45.1	Situations de défaillance.
Serveurs DNS pour l'interface de gestion.	Les serveurs DNS publics OpenDNS, IPv4 : 208.67.220.220, 208.67.222.222; IPv6 : 2620:119:35::35, ou tout ce que vous avez saisi. Les serveurs DNS obtenus à partir du protocole DHCP ne sont jamais utilisés. Firepower 4100/9300 : les serveurs DNS que vous avez définis lors du déploiement du périphérique logique.	Explicite.
Nom d'hôte de gestion.	**firepower** ou tout ce que vous avez saisi. Firepower 4100/9300 : le nom d'hôte que vous avez défini lors du déploiement du périphérique logique.	Explicite.
Accès à la gestion par le biais des interfaces de données.	Une règle de liste d'accès de gestion de l'interface de données permet l'accès HTTPS par le biais de l'interface interne. Les connexions SSH ne sont pas autorisées. Les connexions IPv4 et IPv6 sont autorisées. Firepower 4100/9300 : aucune interface de données n'a de règles d'accès de gestion par défaut. ISA 3000 : aucune interface de données n'a de règles d'accès de gestion par défaut. FTDv : aucune interface de données n'a de règles d'accès de gestion par défaut.	Impliqué.

Paramètres	Configuration	Configuration explicite, implicite ou par défaut
Heure système.	Le fuseau horaire et les serveurs NTP que vous avez sélectionnés. Firepower 4100/9300 : l'heure système est transmise par le châssis. ISA 3000 : serveurs NTP de Cisco : 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org.	Explicite.
Licence Smart.	Soit enregistré avec une licence de base, soit période d'évaluation activée, selon votre sélection. Les licences d'abonnement ne sont pas activées. Accédez à la page des licences Smart pour les activer.	Explicite.
Adresse IP de l'interface interne.	192.168.95.1/24 Firepower 4100/9300 : Les interfaces de données ne sont pas préconfigurées. ISA 3000 : aucune. Vous devez définir l'adresse IP BVI1 manuellement. FTDv : 192.168.45.1/24	Situations de défaillance.
Serveur DHCP pour les clients internes.	Fonctionne sur l'interface interne avec l'ensemble d'adresses 192.168.95.5 à 192.168.95.254. Firepower 4100/9300 : Aucun serveur DHCP activé. ISA 3000 : Aucun serveur DHCP activé. FTDv : L'ensemble d'adresses sur l'interface interne est 192.168.45.46 à 192.168.45.254.	Situations de défaillance.
Configuration automatique DHCP pour les clients internes. (La configuration automatique fournit aux clients des adresses pour les serveurs WINS et DNS.)	Activé sur l'interface externe si vous utilisez DHCP pour obtenir l'adresse IPv4 de l'interface externe. Si vous utilisez l'adressage statique, la configuration automatique DHCP est désactivée.	Explicit, mais indirect.

Paramètres	Configuration	Configuration explicite, implicite ou par défaut
Configuration de l'interface de données.	• 1010 : l'interface externe, Ethernet1/1, est une interface de pare-feu physique. Toutes les autres interfaces sont des ports de commutation qui sont activés et font partie de VLAN1, l'interface interne. Vous pouvez brancher des points terminaux ou des commutateurs dans ces ports et obtenir des adresses du serveur DHCP pour l'interface interne. • Firepower 4100/9300 : toutes les autres interfaces de données sont désactivées. • ISA 3000 : toutes les interfaces de données sont activées et font partie du même groupe de ponts, BVI1. GigabitEthernet1/1 et 1/3 sont des interfaces externes, et GigabitEthernet1/2 et 1/4 sont des interfaces internes. GigabitEthernet 1/1 (externe1) et 1/2 (interne1) et GigabitEthernet 1/3 (externe2) et 1/4 (interne2) (modèles sans fibre uniquement) sont configurés comme paires de contournement matériel. • Tous les autres modèles : les interfaces externe et interne sont les seules configurées et activées. Toutes les autres interfaces de données sont désactivées.	Situations de défaillance.
Adresse IP de l'interface externe.	Il s'agit du port externe par défaut en fonction du modèle de périphérique. Consultez Configuration par défaut avant la configuration initiale, à la page 8. L'adresse IP est obtenue par autoconfiguration DHCP et IPv6, ou il s'agit d'une adresse statique telle qu'elle est saisie (IPv4, IPv6 ou les deux). Firepower 4100/9300 : Les interfaces de données ne sont pas préconfigurées. ISA 3000 : aucune. Vous devez définir l'adresse IP BVI1 manuellement.	L'interface est par défaut. L'adressage est explicite.
Routes statiques.	Si vous configurez une adresse IPv4 ou IPv6 statique pour l'interface externe, une route par défaut statique est configurée pour IPv4/IPv6, le cas échéant, pointant vers la passerelle que vous avez définie pour ce type d'adresse. Si vous sélectionnez DHCP, la voie de routage par défaut est obtenue à partir du serveur DHCP. Des objets réseau sont également créés pour la passerelle et l'adresse « any » (toute), c'est-à-dire 0.0.0.0/0 pour IPv4, ::/0 pour IPv6.	Impliqué.

Paramètres	Configuration	Configuration explicite, implicite ou par défaut
Zones de sécurité.	**inside_zone**, comprenant les interfaces internes. Pour le Firepower 4100/9300, vous devez ajouter des interfaces manuellement à ce périmètre de sécurité. **outside_zone**, contenant les interfaces externes. Pour le Firepower 4100/9300, vous devez ajouter des interfaces manuellement à cette zone. (Vous pouvez modifier ces zones pour ajouter d'autres interfaces ou créer vos propres zones.)	Impliqué.
Politique de contrôle d'accès.	Une règle faisant confiance à tout le trafic de la inside_zone vers la outside_zone. Cela permet sans inspection à tout le trafic des utilisateurs de votre réseau de sortir et à tout le trafic de retour pour ces connexions. L'action par défaut pour tout autre trafic est de le bloquer. Cela empêche tout trafic initié de l'extérieur d'entrer dans votre réseau. Firepower 4100/9300 : il n'y a pas de règles d'accès préconfigurées. ISA 3000 : une règle faisant confiance à tout le trafic de la inside_zone à la outside_zone, et une règle faisant confiance à tout le trafic de la outside_zone à la inside_zone. Trafic non bloqué. Le périphérique dispose également de règles faisant confiance à tout le trafic entre les interfaces de la inside_zone et de la outside_zone. Cela permet, sans inspection, tout le trafic entre les utilisateurs de inside (interne) et entre les utilisateurs de outside (externe).	Impliqué.
NAT	Une règle de PAT dynamique d'interface traduit l'adresse source de tout trafic IPv4 destiné à l'interface externe en un port unique sur l'adresse IP de l'interface externe. Il existe d'autres règles PAT masquées pour activer l'accès HTTPS par le biais des interfaces internes et le routage par les interfaces de données pour l'adresse de gestion. Celles-ci ne s'affichent pas dans le tableau NAT, mais vous les verrez si vous utilisez la commande **show nat** dans l'interface de ligne de commande. Firepower 4100/9300 : la NAT n'est pas préconfigurée. ISA 3000 : la NAT n'est pas préconfigurée.	Impliqué.

Connexion au système

Il y a deux interfaces pour l'appareil Firepower Threat Defense

Interface Web FDM

Le Gestionnaire de périphériques de pare-feu s'exécute dans votre navigateur Web. Vous utilisez cette interface pour configurer, gérer et surveiller le système.

Interface de ligne de commande (CLI, Console)

Utilisez cette interface de ligne de commande pour un dépannage avancé. Vous pouvez également l'utiliser pour la configuration initiale au lieu de Gestionnaire de périphériques de pare-feu.

Les rubriques suivantes expliquent comment vous connecter à ces interfaces et gérer votre compte utilisateur.

Votre rôle d'utilisateur contrôle ce que vous pouvez voir et faire

Votre nom d'utilisateur est assorti d'un rôle, et votre rôle détermine ce que vous pouvez faire ou ce que vous pouvez voir dans le Gestionnaire de périphériques de pare-feu. L'utilisateur **admin** défini localement dispose de tous les privilèges, mais si vous vous connectez à l'aide d'un compte différent, vous pourriez avoir moins de privilèges.

Le coin supérieur droit de la fenêtre Gestionnaire de périphériques de pare-feu affiche votre nom d'utilisateur et votre niveau de privilège.



Les privilèges sont les suivants :

- **Administrateur** : vous pouvez voir et utiliser toutes les fonctionnalités.
- **Utilisateur en lecture-écriture** : vous pouvez faire tout ce qu'un utilisateur en lecture seule peut faire, ainsi que modifier et déployer la configuration. Les seules restrictions concernent les actions critiques pour le système, qui comprennent l'installation des mises à niveau, la création et la restauration de sauvegardes, l'affichage du journal d'audit et la déconnexion d'autres Gestionnaire de périphériques de pare-feu utilisateurs.
- **Utilisateur en lecture seule** : vous pouvez afficher les tableaux de bord et la configuration, mais ne pouvez apporter aucune modification. Si vous tentez d'apporter une modification, le message d'erreur explique que cela est causé par un manque d'autorisation.

Ces privilèges ne sont pas liés à ceux disponibles pour les utilisateurs d'interface de ligne de commande.

Connectez-vous au Gestionnaire de périphériques de pare-feu.

Utilisez le Gestionnaire de périphériques de pare-feu pour configurer, gérer et surveiller le système. Les fonctionnalités que vous pouvez configurer à l'aide du navigateur ne sont pas configurables à l'aide de l'interface de ligne de commande (CLI) ; vous devez utiliser l'interface Web pour mettre en œuvre vos politiques de sécurité.

Utilisez une version actuelle de Firefox, Chrome, Safari, Edge.

Remarque Si vous saisissez le mauvais mot de passe et ne parvenez pas à vous connecter lors de 3 tentatives consécutives, votre compte est verrouillé pendant 5 minutes. Vous devez attendre avant de réessayer de vous connecter.

Avant de commencer

Au départ, vous pouvez vous connecter à Gestionnaire de périphériques de pare-feu en utilisant le nom d'utilisateur **admin** uniquement. Cependant, vous pouvez ensuite configurer l'autorisation pour les utilisateurs supplémentaires définis dans un serveur AAA externe, comme décrit dans Gestion du Gestionnaire de périphériques de pare-feu et accès des utilisateurs Firewall Threat Defense, à la page 843.

Il peut y avoir jusqu'à 5 connexions actives à la fois. Cela inclut les utilisateurs connectés au gestionnaire d'appareil et les sessions API actives, qui sont représentées par des jetons API non expirés. Si vous dépassez cette limite, la session la plus ancienne, soit la connexion au gestionnaire d'appareils ou le jeton API, expirera pour permettre la nouvelle session. Ces limites ne s'appliquent pas aux sessions SSH.

Procédure

Étape 1 À l'aide d'un navigateur, ouvrez la page d'accueil du système, par exemple, https://ftd.example.com.

Vous pouvez utiliser n'importe quelle des adresses suivantes. Vous pouvez utiliser l'adresse IPv4 ou IPv6 ou le nom DNS, si vous en avez configuré un.

- L'adresse IP de gestion.Par défaut (sur la plupart des plateformes), l'interface de gestion est un client DHCP, de sorte que l'adresse IP dépend de votre serveur DHCP.
- L'adresse d'une interface de données que vous avez ouverte pour l'accès HTTPS. Par défaut (sur la plupart des plateformes), l'interface « interne » permet l'accès HTTPS, afin que vous puissiez vous connecter à l'adresse interne par défaut 192.168.95.1. Consultez Configuration par défaut avant la configuration initiale, à la page 8 pour en savoir plus sur l'adresse IP interne de votre modèle.

  Si vous avez modifié le port de données HTTPS, vous devez inclure le port personnalisé dans l'URL. Par exemple, si vous avez changé le port en 4443 : https://ftd.example.com:4443

Astuces

Si votre navigateur n'est pas configuré pour reconnaître le certificat de serveur, vous verrez un avertissement concernant un certificat non fiable. Acceptez le certificat en tant qu'exception ou dans votre magasin de certificats racine de confiance.

Étape 2 Saisissez votre nom d'utilisateur et votre mot de passe définis pour le périphérique, puis cliquez sur **Login (Connexion)**.

Vous pouvez utiliser le nom d'utilisateur **admin**, qui est un utilisateur prédéfini. Pour admin, le mot de passe par défaut est Admin123. Sur AWS, le mot de passe administrateur par défaut est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details** > **(Détails avancés)** > **User Data (Données utilisateur)**) lors du déploiement initial.

Votre session expirera après 30 minutes d'inactivité, et vous serez invité à vous connecter de nouveau. Vous pouvez vous déconnecter en sélectionnant **Log Out** (Déconnexion) dans le menu déroulant de l'icône utilisateur dans le coin supérieur droit de la page.



Connexion avec l'interface de ligne de commande (CLI)

Utilisez l'interface de ligne de commande (CLI) pour configurer le système et effectuer le dépannage de base du système. Vous ne pouvez pas configurer de politiques via une session d'interface de ligne de commande.

Pour vous connecter à l'interface de ligne de commande (CLI), procédez comme suit :

- Utilisez le câble de console fourni avec l'appareil pour connecter votre ordinateur 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. Consultez le guide du matériel de votre appareil pour en savoir plus sur le câble de la console.



Remarque Sur les modèles de périphériques Firepower , l'interface de ligne de commande du port de console est Secure Firewall eXtensible Operating System (FXOS). Pour certains modèles de périphérique, vous pouvez accéder à l'interface de ligne de commande Firepower Threat Defense en utilisant la commande **connect ftd**. Pour Firepower 4100/9300, consultez Se connecter à la console de l'application, à la page 201. Utilisez l'interface de ligne de commande de FXOS uniquement pour le dépannage au niveau du châssis. Utilisez l'interface de ligne de commande de Firepower Threat Defense pour la configuration de base, la surveillance et le dépannage normal du système. Consultez la documentation de FXOS pour obtenir des renseignements sur les commandes FXOS.

- Pour le FTDv, ouvrez la console virtuelle.
- Utilisez un client SSH pour établir une connexion à l'adresse IP de gestion. Vous pouvez également vous connecter à l'adresse sur une interface de données si vous ouvrez l'interface aux connexions SSH (consultez Configuration de la liste d'accès de gestion, à la page 786). L'accès SSH aux interfaces de données est désactivé par défaut. Connectez-vous en utilisant le nom d'utilisateur **admin** ou un autre compte d'utilisateur de l'interface de ligne de commande. Pour admin, le mot de passe par défaut est Admin123. Sur AWS, le mot de passe administrateur par défaut pour le Firewall Threat Defense Virtual est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (détails avancés)** > **User Data (données utilisateur)**) lors du déploiement initial.

Conseils

- Après la connexion, pour des informations sur les commandes disponibles dans l'interface de ligne de commande, entrez **help** ou **?**. Pour obtenir des renseignements sur l'utilisation, consultez Référence de commande Cisco Firepower Threat Defense sur http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.
- Vous pouvez créer des comptes d'utilisateur locaux qui peuvent se connecter à l'interface de ligne de commande à l'aide de la commande **configure user add**. Cependant, ces utilisateurs peuvent uniquement se connecter à l'interface de ligne de commande. Ils ne peuvent pas se connecter à l'interface Web Gestionnaire de périphériques de pare-feu.
- Vous pouvez créer des comptes utilisateur pour l'accès SSH sur un serveur externe. Pour en savoir plus sur la configuration de l'authentification externe pour l'accès SSH, consultez Configuration de l'autorisation externe (AAA) pour les utilisateurs de l'interface de commande (SSH) Firewall Threat Defense, à la page 846.

Modifier votre mot de passe

Vous devez modifier périodiquement votre mot de passe. La procédure suivante explique comment modifier le mot de passe lorsque vous êtes connecté à Gestionnaire de périphériques de pare-feu.

Remarque Si vous êtes connecté à l'interface de ligne de commande, vous pouvez modifier votre mot de passe à l'aide de la commande **configure password**. Vous pouvez modifier le mot de passe d'un autre utilisateur d'interface de ligne de commande avec la commande **configure user password** *username*.

Avant de commencer

Cette procédure s'applique uniquement aux utilisateurs locaux. Si votre compte d'utilisateur est défini sur un serveur AAA externe, vous devez modifier votre mot de passe sur ce serveur.

Procédure

Étape 1 Sélectionnez **Profile** (Profil) dans la liste déroulante de l'icône utilisateur en haut à droite du menu.



Étape 2 Cliquez sur l'onglet **Password** (Mot de passe).

Étape 3 Saisissez votre mot de passe actuel.

Étape 4 Saisissez votre nouveau mot de passe, puis confirmez-le.

Étape 5 Cliquez sur **Change** (Modifier).

Définition des préférences de profil utilisateur

Vous pouvez définir des préférences pour l'interface utilisateur et modifier votre mot de passe.

Procédure

Étape 1 Sélectionnez **Profile** (Profil) dans la liste déroulante de l'icône utilisateur en haut à droite du menu.



Étape 2 Dans l'onglet **Profile** (Profil), configurez les éléments suivants, puis cliquez sur **Save** (Enregistrer).

- **Time Zone for Scheduling Tasks** (Fuseau horaire pour la planification des tâches) : sélectionnez le fuseau horaire que vous souhaitez utiliser pour planifier des tâches telles que les sauvegardes et les mises à jour. Le fuseau horaire du navigateur est utilisé pour les tableaux de bord et les événements, si vous définissez une zone différente.

- **Thème de couleur** : sélectionnez le thème de couleur que vous souhaitez utiliser dans l'interface utilisateur.

Étape 3 Sous l'onglet **Password** (Mot de passe), vous pouvez saisir un nouveau mot de passe et cliquer sur **Change** (Modifier).

Affichage des pages dans d'autres langues que l'anglais

Vous pouvez afficher l'interface graphique et l'aide en ligne dans les langages suivants.

- Chinois
- Anglais (par défaut)
- Japonais
- Coréen

Pour utiliser ces langues, vous devez sélectionner cette langue dans les paramètres de votre navigateur. Il n'y a pas de paramètre de langue dans le produit lui-même.

Si votre navigateur ne prend pas en charge une langue particulière, le produit ne s'affichera pas dans cette langue. Par exemple, la version française ne s'affiche que si vous configurez le navigateur pour utiliser le Français canadien. La sélection d'un autre type de Français permet de laisser le produit en anglais.

Configuration du système

Vous devez effectuer une configuration initiale pour que le système fonctionne correctement dans votre réseau. Un déploiement réussi comprend la connexion correcte des câbles et la configuration des adresses nécessaires pour insérer l'appareil dans votre réseau et le connecter à Internet ou à un autre routeur en amont. La procédure suivante explique le processus de bout en bout.

Avant de commencer

Avant de commencer la configuration initiale, le périphérique comprend certains paramètres par défaut. Pour de plus amples renseignements, consultez la section Configuration par défaut avant la configuration initiale, à la page 8.

Procédure

Étape 1 Connecter les interfaces, à la page 21

Étape 2 Compléter la configuration initiale avec l'assistant d'installation, à la page 23

Pour en savoir plus sur la configuration résultante, consultez Configuration après la configuration initiale, à la page 11.

Connecter les interfaces

La configuration par défaut suppose que certaines interfaces sont utilisées pour les réseaux internes et externes. La configuration initiale sera plus facile à réaliser si vous connectez les câbles réseau aux interfaces en fonction de ces attentes.

La configuration par défaut de la plupart des modèles est conçue pour vous permettre de connecter votre ordinateur de gestion à l'interface interne. Sinon, vous pouvez également connecter directement votre station de travail au port de gestion. Les interfaces sont sur des réseaux différents, alors n'essayez pas de connecter les interfaces internes et le port de gestion sur le même réseau.

Ne connectez aucune des interfaces internes à un réseau doté d'un serveur DHCP actif. Cela entre en conflit avec le serveur DHCP qui fonctionne déjà sur l'interface interne Si vous souhaitez utiliser un autre serveur DHCP pour le réseau, désactivez le serveur DHCP indésirable après la configuration initiale.

Consultez le guide de démarrage de votre modèle pour obtenir les schémas de câblage.

(Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande

Si vous ne pouvez pas utiliser l'adresse IP de gestion par défaut, vous pouvez vous connecter au port de console et effectuer la configuration initiale au niveau de l'interface de ligne de commande, y compris la définition de l'adresse IP de gestion, de la passerelle et d'autres paramètres réseau de base. Vous ne pouvez configurer que les paramètres de l'interface de gestion; vous ne pouvez pas configurer d'interfaces internes ou externes, que vous pouvez configurer ultérieurement dans l'interface graphique.

Remarque Vous n'avez pas besoin d'utiliser cette procédure pour Firepower 4100/9300, car vous définissez l'adresse IP manuellement lors du déploiement.

Remarque Vous ne pouvez pas relancer le script de configuration de l'interface de ligne de commande à moins d'effacer la configuration; par exemple, en recréant l'image. Cependant, tous ces paramètres peuvent être modifiés ultérieurement au niveau de l'interface de ligne de commande à l'aide des commandes **configure network**. Consultez *Référence des commandes de défense contre les menaces de Cisco Secure Firewall*.

Procédure

Étape 1 Connexion au port de la console Firewall Threat Defense. Consultez Connexion avec l'interface de ligne de commande (CLI), à la page 18 pour de plus amples renseignements.

Étape 2 Connectez-vous avec le nom d'utilisateur **admin**.

Pour admin, le mot de passe par défaut est Admin123. Sur AWS, le mot de passe administrateur par défaut pour le Firewall Threat Defense Virtual est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (détails avancés)** > **User Data (données utilisateur)**) lors du déploiement initial.

Étape 3 La première fois que vous vous connectez à Firewall Threat Defense , vous êtes invité à accepter le contrat de licence de l'utilisateur final (cLUF) et à changer le mot de passe de l'administrateur. Vous verrez ensuite le script de configuration de l'interface de ligne de commande.

Les valeurs par défaut ou les valeurs saisies précédemment apparaissent entre parenthèses. Pour accepter les valeurs saisies précédemment, appuyez sur la touche **Entrée**.

Consultez les consignes suivantes :

- **Enter the IPv4 default gateway for the management interface** (saisissez la passerelle IPv4 par défaut pour l'interface de gestion). Si vous définissez une adresse IP manuelle, saisissez les interfaces de données (**data-interfaces**) ou l'adresse IP du routeur de passerelle. Le paramètre **data-interfaces** envoie le trafic de gestion sortant sur le fond de panier pour quitter une interface de données. Ce paramètre est utile si vous ne disposez pas d'un réseau de gestion distinct pouvant accéder à Internet. Le trafic provenant de l'interface de gestion comprend l'enregistrement des licences et les mises à jour de base de données qui nécessitent un accès Internet. Si vous utilisez des **data-interfaces (interfaces de données)**, vous pouvez toujours utiliser le Gestionnaire de périphériques de pare-feu (ou SSH) sur l'interface de gestion si vous êtes directement connecté au réseau de gestion, mais pour la gestion à distance de réseaux ou d'hôtes particuliers, vous devez ajouter une route statique à l'aide de la commande **configure network static-routes**. Notez que la gestion du Gestionnaire de périphériques de pare-feu sur les interfaces de données n'est pas touchée par ce paramètre. Si vous utilisez DHCP, le système utilise la passerelle fournie par DHCP et utilise les interfaces de données (**data-interfaces**) comme méthode de secours si DHCP ne fournit pas de passerelle.
- **If your networking information has changed, you will need to reconnect** (si vos informations réseau ont changé, vous devrez vous reconnecter) : Si vous êtes connecté avec SSH à l'adresse IP par défaut, mais que vous avez changé l'adresse IP au moment de la configuration initiale, vous serez déconnecté. Reconnectez-vous avec la nouvelle adresse IP et le nouveau mot de passe. Les connexions à la console ne sont pas touchées.
- **Gérer l'appareil localement?** : saisissez **oui** pour utiliser Gestionnaire de périphériques de pare-feu. Une réponse **non** signifie que vous avez l'intention d'utiliser le système Centre de gestion Firepower (FMC) pour gérer le dispositif.

Exemple :

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
```

```
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

Étape 4 Connectez-vous à Gestionnaire de périphériques de pare-feu sur la nouvelle adresse IP de gestion.

Compléter la configuration initiale avec l'assistant d'installation

Lorsque vous vous connectez pour la première fois à Gestionnaire de périphériques de pare-feu, vous êtes guidé au moyen de l'assistant d'installation de l'appareil pour compléter la configuration initiale du système.

Si vous envisagez d'utiliser l'appareil selon une configuration à haute disponibilité, veuillez lire Préparer les deux unités pour la haute disponibilité, à la page 216.

Remarque Firepower 4100/9300 et ISA 3000 ne prennent pas en charge l'assistant de configuration. Cette procédure ne s'applique donc pas à ces modèles. Pour Firepower 4100/9300, toute la configuration initiale est définie lorsque vous déployez le périphérique logique à partir du châssis. Pour l'ISA 3000, une configuration spéciale par défaut est appliquée avant l'expédition.

Avant de commencer

Assurez-vous de relier une interface de données avec votre périphérique de passerelle, par exemple un modem câble ou un routeur. Pour les déploiements en périphérie, il s'agit de votre passerelle Internet. Pour les déploiements de centres de données, il s'agirait d'un routeur principal. Utilisez l'interface « externe » par défaut pour votre modèle (voir Connecter les interfaces, à la page 21et Configuration par défaut avant la configuration initiale, à la page 8).

Ensuite, reliez votre ordinateur de gestion à l'interface « interne » de votre modèle de matériel. Sinon, vous pouvez vous connecter à l'interface de gestion. Pour le Firewall Threat Defense Virtual, assurez-vous simplement que vous avez une connexion à l'adresse IP de gestion.

(Sauf pour le Firewall Threat Defense Virtual, ce qui nécessite une connectivité à Internet à partir de l'adresse IP du gestionnaire.) Une connexion entre l'interface de gestion et le réseau n'est pas nécessaire. Par défaut, le système obtient les licences système, les mises à jour de base de données et les autres mises à jour par le biais des interfaces de données (généralement l'interface externe) qui se connectent à Internet. Si vous souhaitez plutôt utiliser un réseau de gestion distinct, vous pouvez relier l'interface de gestion à un réseau et configurer une passerelle de gestion distincte une fois la configuration initiale terminée.

Pour modifier les paramètres réseau de l'interface de gestion si vous ne pouvez pas accéder à l'adresse IP par défaut, consultez (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 21.

Procédure

Étape 1 Connectez-vous à Gestionnaire de périphériques de pare-feu.

a) En supposant que vous n'êtes pas passé par la configuration initiale dans l'interface de ligne de commande, ouvrez le Gestionnaire de périphériques de pare-feu à **https://***l'adresse IP*, où l'adresse est l'une des suivantes.

- Pour une connexion avec l'interface interne : **https://192.168.95.1**.
- (rle Firewall Threat Defense Virtual) Si vous êtes connecté à l'interface de gestion :**https://192.168.45.45**.
- (Tous les autres modèles) Pour une connexion avec l'interface de gestion : **https://***dhcp_client_ip*.

b) Connectez-vous avec le nom d'utilisateur **admin**. Pour admin, le mot de passe par défaut est Admin123. Sur AWS, le mot de passe administrateur par défaut pour le Firewall Threat Defense Virtual est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (détails avancés)** > **User Data (données utilisateur)**) lors du déploiement initial.

Étape 2 S'il s'agit de la première connexion au système et que vous n'avez pas utilisé l'assistant de configuration au niveau de l'interface de ligne de commande, vous devrez lire et accepter le contrat de licence d'utilisateur final et modifier le mot de passe de l'administrateur.

Vous devez suivre ces étapes pour continuer.

Étape 3 Configurez les options suivantes pour l'interface externe et l'interface de gestion, puis cliquez sur **Next** (suivant).

Mise en garde
Vos paramètres sont déployés sur l'appareil lorsque vous cliquez sur **Next** (suivant). L'interface sera désignée comme « externe » et sera ajoutée à la zone de sécurité « outside_zone ». Vérifiez que vos paramètres sont corrects.

Interface externe

- **Configure IPv4** (configuration de l'adresse IPv4) : l'adresse IPv4 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un masque de sous-réseau et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv4. Ne configurez pas l'adresse IP sur le même sous-réseau que l'adresse interne par défaut (voir Configuration par défaut avant la configuration initiale, à la page 8), que ce soit de manière statique ou par le biais du protocole DHCP. Vous ne pouvez pas configurer PPPoE à l'aide de l'assistant de configuration. PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous pouvez configurer PPPoE une fois que l'installation de l'assistant est terminée. Consultez Configurer une interface physique, à la page 256.
- **Configure IPv6** (configuration de l'adresse IPv6) : l'adresse IPv6 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un préfixe et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv6.

Interface de gestion

- **DNS Servers** (serveurs DNS) : le serveur DNS pour l'adresse de gestion du système. Entrez une ou plusieurs adresses de serveurs DNS pour la résolution de noms. Par défaut, les serveurs DNS publics OpenDNS ou les serveurs DNS que vous obtenez du serveur DHCP sont sélectionnés. Si vous modifiez les champs et souhaitez revenir à la valeur par défaut, cliquez sur **Use OpenDNS** (utiliser OpenDNS) pour recharger les adresses IP appropriées dans les champs. Votre fournisseur de services Internet peut exiger que vous utilisiez des serveurs DNS spécifiques. Si, après avoir terminé l'installation avec

l'assistant, vous trouvez que la résolution DNS ne fonctionne pas, consultez Dépannage du DNS pour l'interface de gestion, à la page 858.

- **Firewall Hostname** (nom d'hôte du pare-feu) : le nom d'hôte de l'adresse de gestion du système.

Étape 4 Configurez les paramètres d'heure du système et cliquez sur **Next** (suivant).

- **Time Zone** (fuseau horaire) : sélectionnez le fuseau horaire pour le système.
- **NTP Time Server** (serveur horaire NTP) : sélectionnez cette option pour utiliser les serveurs NTP par défaut ou pour saisir manuellement les adresses de vos serveurs NTP. Vous pouvez ajouter plusieurs serveurs pour fournir des sauvegardes.

Étape 5 Configurez les licences Smart pour le système.

Vous devez avoir un compte de licence Smart pour obtenir et appliquer les licences requises par le système. Au départ, vous pouvez utiliser la licence d'évaluation de 90 jours, puis configurer les licences Smart ultérieurement.

Pour enregistrer le périphérique dès maintenant, sélectionnez l'option pour enregistrer le périphérique, cliquez sur le lien pour vous connecter à votre compte Smart Software Manager, générez un nouveau jeton et copiez le jeton dans la zone d'édition. Vous devez également sélectionner votre région de services et décider d'envoyer ou non les données d'utilisation au Réseau de succès Cisco (Cisco Success Network). Le texte à l'écran explique ces paramètres plus en détail.

Si vous ne souhaitez pas encore enregistrer l'appareil, sélectionnez l'option du mode d'évaluation (evaluation mode). La période d'évaluation dure jusqu'à 90 jours. Pour enregistrer ultérieurement l'appareil et obtenir des licences intelligentes, cliquez sur **Device (périphérique)**, puis cliquez sur le lien dans le groupe des licences Smart (**Smart Licenses**).

Étape 6 Cliquez sur **Finish** (Terminer).

Prochaine étape

- Si vous souhaitez utiliser les fonctionnalités couvertes par les licences facultatives, comme le filtrage d'URL par catégorie, l'inspection des intrusions ou la prévention des logiciels malveillants, activez les licences requises. Consultez Activation ou désactivation des licences facultatives, à la page 95.
- Connectez les autres interfaces de données à des réseaux distincts et configurez les interfaces. Pour en savoir plus sur la configuration des interfaces, consultez Comment ajouter un sous-réseau, à la page 73 et Interfaces, à la page 251.
- Si vous gérez le périphérique via l'interface interne et que vous souhaitez ouvrir des sessions d'interface de ligne de commande via l'interface interne, ouvrez l'interface interne aux connexions SSH. Consultez Configuration de la liste d'accès de gestion, à la page 786.
- Parcourez les scénarios d'utilisation pour apprendre comment utiliser le produit. Consultez Meilleures pratiques : scénarios d'utilisation pour Firewall Threat Defense, à la page 43.

Que faire si vous n'obtenez pas d'adresse IP pour l'interface externe

La configuration par défaut du périphérique comprend une adresse IPv4 statique pour l'interface interne. Vous ne pouvez pas modifier cette adresse au moyen de l'assistant de configuration initiale du périphérique, bien que vous puissiez la modifier par la suite.

L'adresse IP interne par défaut peut entrer en conflit avec d'autres réseaux connectés au périphérique. Cela est particulièrement vrai si vous utilisez DHCP sur l'interface externe pour obtenir une adresse de votre fournisseur de services Internet. Certains fournisseurs de services Internet utilisent le même sous-réseau que le réseau interne comme ensemble d'adresses. Comme vous ne pouvez pas avoir deux interfaces de données avec des adresses sur le même sous-réseau, les adresses en conflit du fournisseur de services Internet ne peuvent pas être configurées sur l'interface externe.

En cas de conflit entre l'adresse IP statique interne et l'adresse fournie par DHCP sur l'interface externe, le diagramme de connexion doit afficher l'interface externe comme étant administrativement opérationnelle, mais sans adresse IPv4.

L'assistant de configuration terminera avec succès dans ce cas, et toutes les politiques et paramètres de NAT, d'accès et d'autres politiques et paramètres par défaut seront configurés. Suivez simplement la procédure ci-dessous pour éliminer le conflit.

Avant de commencer

Vérifiez que vous avez une bonne connexion avec le fournisseur de services Internet. Bien qu'un conflit de sous-réseau vous empêche d'obtenir une adresse sur l'interface externe, vous ne parviendrez pas à en obtenir une si vous n'avez tout simplement pas de lien avec le fournisseur de services Internet.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis sur le lien dans le résumé des **Interfaces**.

Étape 2 Passez la souris sur la colonne **Actions** pour l'interface interne et cliquez sur l'icône de modification ( ).

Étape 3 Dans l'onglet **IPv4 Address**, entrez une adresse statique sur un sous-réseau unique, par exemple 192.168.2.1/24 ou 192.168.46.1/24. Notez que l'adresse de gestion par défaut est 192.168.45.45/24. Par conséquent, n'utilisez pas ce sous-réseau.

Vous avez également la possibilité d'utiliser DHCP pour obtenir une adresse si vous avez déjà un serveur DHCP sur le réseau interne. Cependant, vous devez d'abord cliquer sur **Delete** (Supprimer) dans le groupe **DHCP SERVER IS DEFINED FOR THIS INTERFACE** (LE SERVEUR DHCP EST DÉFINI POUR CETTE INTERFACE) afin de supprimer le serveur DHCP de l'interface.

Étape 4 Dans la zone **DHCP SERVER IS DEFINED FOR THIS INTERFACE** (LE SERVEUR DHCP EST DÉFINI POUR CETTE INTERFACE), cliquez sur **Edit** (Modifier) et modifiez le regroupement DHCP en une plage sur le nouveau sous-réseau, par exemple, 192.168.2.5-192.168.2.254.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications apportées à l'interface.

Étape 6 Cliquez sur le bouton **Deploy** (déployer) dans le menu pour déployer vos modifications.



Étape 7 Cliquez sur **Deploy Now** (déployer maintenant).

Une fois le déploiement terminé, le graphique de connexion devrait afficher que l'interface externe dispose maintenant d'une adresse IP. Utilisez un client sur le réseau interne pour vérifier que vous avez une connectivité à Internet ou à un autre réseau en amont.

Bases de la configuration

Les rubriques suivantes expliquent les méthodes de base pour la configuration du périphérique.

Configuration du périphérique

Lorsque vous vous connectez pour la première fois à Gestionnaire de périphériques de pare-feu, vous êtes guidé dans un assistant de configuration pour vous aider à configurer les paramètres de base. Une fois que vous avez terminé l'assistant, utilisez la méthode suivante pour configurer les autres fonctionnalités et gérer la configuration du périphérique.

Si vous avez du mal à dissocier visuellement les éléments, sélectionnez un schéma de couleur différent dans le profil d'utilisateur. Sélectionnez **Profile** (Profil) dans le menu déroulant de l'icône utilisateur dans le coin supérieur droit de la page.



Procédure

Étape 1 Cliquez sur **Device (périphérique)** pour accéder au **Device Summary (Résumé du périphérique)**.

Le tableau de bord affiche un état visuel du périphérique, y compris les interfaces activées et si les paramètres de clé sont configurés (en vert) ou doivent toujours être configurés. Pour en savoir plus, consultez Affichage de l'interface et de l'état de gestion, à la page 33.

Au-dessus de l'image d'état se trouve un résumé du modèle de périphérique, de la version du logiciel, de la version VDB (système et base de données relative aux vulnérabilités) et des dernières règles de prévention des intrusions mises à jour. Cette zone affiche aussi l'état de la haute disponibilité, y compris des liens pour configurer la fonctionnalité ; voir Haute disponibilité (basculement), à la page 203. Elle affiche également l'état d'enregistrement dans le nuage, où vous voyez le compte auquel le périphérique est inscrit si vous utilisez la gestion en nuage ; voir Configuration de Cisco Cloud Services, à la page 809.

Sous l'image se trouvent des groupes pour les différentes fonctionnalités que vous pouvez configurer, avec des résumés des configurations dans chaque groupe et des actions que vous pouvez effectuer pour gérer la configuration du système.

Étape 2 Cliquez sur les liens dans chaque groupe pour configurer les paramètres ou effectuer les actions.

Voici un résumé des groupes :

- **Interface** : vous devez avoir au moins deux interfaces de données configurées en plus de l'interface de gestion. Consultez Interfaces, à la page 251.
- **Routing (Routage)** : la configuration du routage. Vous devez définir une route par défaut. D'autres routes peuvent être nécessaires selon votre configuration. Consultez Routage, à la page 313.
- **Updates** (Mises à jour) : mises à jour de géolocalisation, des règles de prévention des intrusions et de la base de données des vulnérabilités, ainsi que mises à niveau du logiciel système. Configurez un calendrier de mises à jour régulières afin de vous assurer de disposer des dernières mises à jour de base de données si vous utilisez ces fonctionnalités. Vous pouvez également accéder à cette page si vous devez télécharger

une mise à jour avant l'exécution de la mise à jour planifiée. Consultez Mise à jour des bases de données système et des flux, à la page 819.

- **System Settings** (Paramètres système) : ce groupe comprend divers paramètres. Certains sont des paramètres de base que vous configurez lors de la configuration initiale du périphérique, puis que vous modifiez rarement. Consultez Paramètres système, à la page 785.
- **Smart License** (Licence Smart) : affiche l'état actuel des licences du système. Vous devez installer les licences appropriées pour utiliser le système. Certaines fonctionnalités nécessitent des licences particulières. Consultez Octroi de licence du système, à la page 87.
- **Backup and Restore** (Sauvegarde et restauration) : sauvegardez la configuration du système ou restaurez une sauvegarde précédente. Consultez Sauvegarde et restauration du système, à la page 830.
- **Troubleshoot** (Dépannage) : générez un fichier de dépannage à la demande du centre d'assistance technique de Cisco. Consultez Création d'un fichier de dépannage, à la page 863.
- **Site-to-Site VPN** (VPN de site à site) : connexions de réseau privé virtuel (VPN) de site à site entre ce périphérique et des périphériques distants. Consultez Gestion des VPN de site à site, à la page 667.
- **Remote Access VPN** (VPN d'accès à distance) : configuration de réseau privé virtuel (VPN) d'accès à distance qui permet à des clients externes de se connecter à votre réseau interne. Consultez Configuration du VPN d'accès à distance, à la page 711.
- **Advanced Configuration** (Configuration avancée) : utilisez FlexConfig et Smart CLI pour configurer des fonctionnalités que vous ne pouvez pas configurer autrement à l'aide de Gestionnaire de périphériques de pare-feu. Consultez Configuration avancée, à la page 869.
- **Device Administration** (Administration du périphérique) : affichez le journal d'audit ou exportez une copie de la configuration. Consultez Audit et gestion du changement, à la page 836.

Étape 3 Cliquez sur le bouton **Deploy** (déployer) dans le menu pour déployer vos modifications.



Les modifications ne sont actives sur le périphérique que lorsque vous les déployez. Consultez Déploiement des modifications, à la page 30.

Prochaine étape

Cliquez sur **Policies** (Politiques) dans le menu principal et configurez la politique de sécurité pour le système. Vous pouvez également cliquer sur **Objects** (Objets) pour configurer les objets nécessaires dans ces politiques.

Configuration des politiques de sécurité

Utilisez les politiques de sécurité pour mettre en œuvre la politique d'utilisation acceptable de votre entreprise et pour protéger votre réseau contre les intrusions et les autres menaces.

Procédure

Étape 1 Cliquez sur **Policies** (Politiques).

La page Security Policies (Politiques de sécurité) affiche le flux général d'une connexion dans le système et l'ordre dans lequel les politiques de sécurité sont appliquées.

Étape 2 Cliquez sur le nom d'une politique et configurez-la.

Vous n'aurez peut-être pas besoin de configurer chaque type de politique, bien que vous deviez toujours avoir une politique de contrôle d'accès. Voici un résumé des politiques :

- **Déchiffrement SSL** : Si vous souhaitez inspecter les connexions chiffrées (comme HTTPS) pour détecter les intrusions, les logiciels malveillants, etc., vous devez déchiffrer les connexions. Utilisez la politique de déchiffrement SSL pour déterminer les connexions qui doivent être déchiffrées. Le système rechiffre la connexion après l'avoir inspectée. Consultez Configuration des politiques de déchiffrement SSL, à la page 456.
- **Identité** : Si vous souhaitez corréler l'activité du réseau à des utilisateurs individuels ou contrôler l'accès au réseau en fonction de l'utilisateur ou de l'appartenance à un groupe d'utilisateurs, utilisez la politique d'identité pour déterminer l'utilisateur associé à une adresse IP source donnée. Consultez Configuration des politiques d'identité, à la page 478.
- **Security Intelligence** (Renseignements sur la sécurité) : utilisez la politique sur les renseignements sur la sécurité pour supprimer rapidement les connexions en provenance des adresses IP ou des URL de la liste de blocage ou vers celles-ci. En inscrivant sur la liste de blocage les mauvais sites connus, vous n'avez pas besoin de les prendre en compte dans votre politique de contrôle d'accès. Cisco fournit des flux régulièrement mis à jour d'adresses et d'adresses URL incorrectes afin que la liste de blocage issue des renseignements sur la sécurité se mette à jour de façon dynamique. En utilisant les flux, vous n'avez pas besoin de modifier la politique pour ajouter ou supprimer des éléments dans la liste de blocage. Consultez Configurer les renseignements sur la sécurité, à la page 494.
- **NAT** (Network Address Translation, traduction d'adresses réseau) : utilisez la politique NAT pour convertir les adresses IP internes en adresses de routage externe. Consultez Configurer la traduction d'adresses réseau (NAT), à la page 578.
- **Contrôle d'accès** : Utilisez la politique de contrôle d'accès pour déterminer les connexions autorisées sur le réseau. Vous pouvez procéder au filtrage selon la zone de sécurité, l'adresse IP, le protocole, le port, l'application, l'adresse URL, l'utilisateur ou le groupe d'utilisateurs. Vous pouvez aussi appliquer également des politiques en lien avec la prévention des intrusions et avec la présence de fichiers (logiciels malveillants) en utilisant des règles de contrôle d'accès. Utilisez cette politique pour mettre en œuvre le filtrage d'URL. Consultez Configuration de la politique de contrôle d'accès, à la page 515.
- **Intrusion** : Utilisez les politiques de prévention des intrusions pour rechercher les menaces connues. Bien que vous appliquiez des politiques de prévention des intrusions à l'aide de règles de contrôle d'accès, vous pouvez modifier lesdites politiques pour activer ou désactiver sélectivement des règles de prévention précises en lien avec les intrusions. Consultez Stratégies de prévention des intrusions , à la page 539.

Étape 3 Cliquez sur le bouton **Deploy** (déployer) dans le menu pour déployer vos modifications.



Les modifications ne sont actives sur le périphérique que lorsque vous les déployez. Consultez Déploiement des modifications, à la page 30.

Recherche de règles ou d'objets

Vous pouvez utiliser la recherche en texte intégral sur des listes de règles de politique ou d'objets pour vous aider à trouver l'élément que vous souhaitez modifier. Cela est particulièrement utile lorsqu'il s'agit de politiques qui ont des centaines de règles ou de longues listes d'objets.

La méthode d'utilisation de la recherche sur les règles et les objets est la même pour tout type de politique (à l'exception de la politique de prévention des intrusions) ou d'objet : dans le champ **Search (Rechercher)**, saisissez une chaîne à trouver, puis appuyez sur Enter (Entrée).

Cette chaîne peut exister dans n'importe quelle partie de la règle ou de l'objet, et elle peut être partielle. Vous pouvez utiliser l'astérisque * comme caractère générique pour correspondre à zéro ou à plusieurs caractères. N'incluez pas les caractères suivants, ils ne sont pas pris en charge dans la chaîne de recherche : ?~!{}<>:%. Les caractères suivants sont ignorés : ;#&.

La chaîne peut apparaître dans un objet du groupe. Par exemple, vous pouvez saisir une adresse IP et rechercher les objets ou les groupes réseau qui précisent cette adresse.

Lorsque vous avez terminé, cliquez sur le **x** à droite de la zone de recherche pour effacer le filtre.

Déploiement des modifications

Lorsque vous mettez à jour une politique ou un paramètre, la modification n'est pas immédiatement appliquée au périphérique. Il existe un processus en deux étapes :

1. Apportez vos modifications.
2. Déployez vos modifications.

Ce processus vous permet d'apporter un groupe de modifications connexes sans vous obliger à exécuter un périphérique d'une manière « partiellement configurée ». Dans la plupart des cas, le déploiement inclut uniquement vos modifications. Toutefois, si nécessaire, le système réappliquera l'ensemble de la configuration, ce qui pourrait perturber votre réseau. En outre, certaines modifications nécessitent le redémarrage des moteurs d'inspection, avec une diminution du trafic lors du redémarrage. Ainsi, envisagez de déployer des modifications lorsque les perturbations potentielles auront le moins d'impact.

Remarque Si la tâche de déploiement échoue, le système doit restaurer toutes les modifications partielles de la configuration précédente. La restauration comprend l'effacement de la configuration du plan de données et le redéploiement de la version précédente. Cela perturbera le trafic jusqu'à la fin de la restauration.

Après avoir terminé les modifications que vous souhaitez apporter, utilisez la procédure suivante pour les déployer sur le périphérique.

Mise en garde Le périphérique Firewall Threat Defense abandonne le trafic lorsque les moteurs d'inspection sont occupés en raison d'un problème de ressources logicielles ou en panne en raison d'une configuration nécessitant le redémarrage des moteurs pendant le déploiement de la configuration. Pour des informations détaillées sur les modifications nécessitant un redémarrage, consultez Changements de configuration qui redémarrent les moteurs d'inspection., à la page 32.

Procédure

Étape 1 Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

L'icône est mise en évidence avec un point lorsqu'il y a des modifications non déployées.



La fenêtre Pending Changes (modifications en attente) affiche une comparaison de la version déployée de la configuration avec les modifications en attente. Ces modifications sont codées par couleur pour indiquer les éléments supprimés, ajoutés ou modifiés. Consultez la légende dans la fenêtre pour obtenir une explication des couleurs.

Si le déploiement nécessite le redémarrage des moteurs d'inspection, la page comprend un message qui fournit des détails sur les modifications qui nécessitent un redémarrage. Si la perte de trafic momentanée à ce moment est inacceptable, fermez la boîte de dialogue et attendez un meilleur moment pour déployer les modifications.

Si l'icône n'est pas en surbrillance, vous pouvez toujours cliquer dessus pour voir la date et l'heure de la dernière tâche de déploiement réussie. Il existe également un lien pour vous afficher l'historique de déploiement, qui vous mène vers la page d'audit filtrée pour afficher uniquement les tâches de déploiement.



Étape 2 Si vous êtes satisfait des modifications, vous pouvez cliquer sur **Deploy Now** (déployer maintenant) pour lancer le travail immédiatement.

La fenêtre montrera que le déploiement est en cours. Vous pouvez fermer la fenêtre ou attendre la fin du déploiement. Si vous fermez la fenêtre alors que le déploiement est en cours, le travail ne s'arrête pas. Vous pouvez voir les résultats dans la liste des tâches ou dans le journal d'audit. Si vous laissez la fenêtre ouverte, cliquez sur le lien **Deployment History** (historique de déploiement) pour afficher les résultats.

Vous pouvez également effectuer les opérations suivantes :

- **Name the Job** (Nommer la tâche) : pour nommer la tâche de déploiement, cliquez sur la flèche déroulante sur le bouton **Deploy Now** (Déployer maintenant) et sélectionnez **Name the Deployment Job** (Nommer la tâche de déploiement). Saisissez un nom, puis cliquez sur **Deploy** (Déployer). Le nom s'affichera dans Audit et dans Deployment History (Historique des déploiements) en tant qu'élément de la tâche, ce qui pourrait vous aider à la retrouver plus facilement.

  Par exemple, si vous nommez une tâche « Configuration de l'interface DMZ », un déploiement réussi sera nommé « Déploiement terminé : Configuration de l'interface DMZ ». De plus, le nom est utilisé comme Event Name (Nom de l'événement) dans les événements Task Started (Tâche démarrée) et Task Completed (Tâche terminée) associés à la tâche de déploiement.

- **Discard Changes** (Supprimer les modifications) : pour supprimer toutes les modifications en attente, cliquez sur **More Options (Plus d'options)** > **Discard All (Supprimer tout)**. Vous êtes invité à confirmer.
- **Copy Changes** (Copier les modifications) : pour copier la liste des modifications dans le presse-papier, cliquez sur **More Options (Plus d'options)** > **Copy to Clipboard (Copier dans le presse-papiers)**. Cette option fonctionne uniquement s'il y a moins de 500 modifications.
- **Download Changes** (Télécharger les modifications) : pour télécharger la liste des modifications sous forme de fichier, cliquez sur **More Options (Plus d'options)** > **Download as Text (Télécharger en tant que texte)**. Vous êtes invité à enregistrer le fichier sur votre poste de travail. Il utilise le format YAML. Vous pouvez l'afficher dans un éditeur de texte si vous n'avez pas d'éditeur prenant spécifiquement en charge le format YAML.

Changements de configuration qui redémarrent les moteurs d'inspection.

N'importe laquelle des configurations ou actions suivantes redémarre les moteurs d'inspection lorsque vous déployez des modifications de configuration.

⚠

Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations nécessite le redémarrage des moteurs d'inspection, ce qui interrompt l'inspection du trafic et entraîne une perte de trafic.

Déploiement

Certaines modifications requièrent le redémarrage des plateformes d'inspection, ce qui entraînera une perte de trafic momentanée. Voici les modifications qui requièrent le redémarrage de la plateforme d'inspection :

- La politique de déchiffrement SSL est activée ou désactivée.
- La MTU a été modifiée sur au moins une interface physique (mais pas les sous-interfaces).
- Vous ajoutez ou supprimez une politique de fichiers dans une règle de contrôle d'accès.
- La VDB a été mise à jour.
- Création ou interruption de la configuration à haute disponibilité.

En outre, certains paquets peuvent être abandonnés lors du déploiement si le processus Snort est occupé, avec une utilisation totale de l'UC dépassant 60 %. Vous pouvez vérifier l'utilisation actuelle de l'UC pour Snort à l'aide de la commande **show asp inspect-dp snort**.

Mises à jour des bases de données du système

Si vous téléchargez une mise à jour de la base de données des règles ou de la VDB, vous devez déployer la mise à jour pour qu'elle devienne active. Ce déploiement peut redémarrer les moteurs d'inspection. Lorsque vous téléchargez manuellement une mise à jour ou planifiez une mise à jour, vous pouvez indiquer si le système doit déployer automatiquement les modifications une fois le téléchargement terminé. Si le système ne déploie pas automatiquement la mise à jour, la mise à jour est appliquée lors du prochain déploiement de modifications, auquel cas les moteurs d'inspection pourraient redémarrer.

Mises à jour du système

L'installation d'une mise à jour ou d'un correctif du système qui ne redémarre pas le système et comprend une modification binaire nécessite le redémarrage des moteurs d'inspection. Les modifications binaires peuvent inclure des modifications des moteurs d'inspection, d'un préprocesseur, de la base de données relative aux vulnérabilités (VDB) ou d'une règle d'objet partagé. Notez également qu'un correctif qui n'inclut pas de modification binaire peut parfois nécessiter un redémarrage Snort.

Modifications de configuration qui forcent un déploiement complet

Dans la plupart des cas, le déploiement inclut uniquement vos modifications. Toutefois, si nécessaire, le système réappliquera l'ensemble de la configuration, ce qui pourrait perturber votre réseau. Voici quelques modifications qui forcent un déploiement complet.

- Les politiques de renseignements de sécurité ou d'identité sont initialement activées.
- Les politiques de renseignements de sécurité et d'identité sont désactivées.
- Création d'un EtherChannel lorsque vous réutilisez des données.
- Suppression d'un EtherChannel.
- Modification des associations d'interfaces membres d'un EtherChannel.
- Suppression de toute interface utilisée dans la configuration. Par exemple, suppression d'une sous-interface qui fait partie d'un périmètre de sécurité utilisé par une règle de contrôle d'accès.
- Modification d'un objet FlexConfig qui fait partie de la politique FlexConfig ou suppression d'un objet de la politique, lorsque cet objet ne comprend pas de lignes de négation. L'omission des lignes de négation force le système à un déploiement complet, car il n'y a aucun moyen spécifique de supprimer la configuration produite par l'objet FlexConfig. Vous pouvez éviter ce problème en insérant toujours les lignes de négation appropriées dans chaque objet FlexConfig.

Affichage de l'interface et de l'état de gestion

Le résumé du périphérique comprend une vue graphique de votre périphérique et la sélection des paramètres pour l'adresse de gestion. Pour ouvrir le Device Summary (Résumé du périphérique, cliquez sur **Device** (Périphérique).

Les éléments de ce graphique changent de couleur en fonction de l'état de l'élément. Le fait de passer le curseur sur des éléments fournit parfois des informations supplémentaires. Utilisez ce graphique pour surveiller les éléments suivants.



Remarque La partie interface du graphique, y compris les informations sur l'état de l'interface, est également disponible sur la page **Interfaces** et dans le tableau de bord **de surveillance** > **du système**.

État d'interface

Passez le curseur sur un port pour voir ses adresses IP et ses états d'activation et de liaison. Les adresses IP peuvent être attribuées statiquement ou obtenues à l'aide de DHCP. Le déplacement sur une interface virtuelle de pont (BVI) affiche également la liste des interfaces membres.

Les ports d'interface utilisent le code de couleur suivant :

- Vert — l'interface est configurée, activée et la liaison est activée.
- Gris — l'interface n'est pas activée.
- Orange/rouge — l'interface est configurée et activée, mais la liaison est en panne. Si l'interface est câblée, il s'agit d'une condition d'erreur qui doit être corrigée. Si l'interface n'est pas câblée, il s'agit de l'état attendu.

Connexions de réseau internes et externes

Le graphique indique quel port est connecté aux réseaux externe (ou en amont) et interne, dans les conditions suivantes.

- Réseau interne : le port du réseau interne est affiché pour l'interface nommée « inside » (interne) uniquement. S'il existe d'autres réseaux internes, ils ne sont pas affichés. Si vous ne nommez aucune interface « inside », aucun port n'est marqué comme port interne.
- Réseau externe : le port du réseau externe est affiché pour l'interface nommée « outside » (externe) uniquement. Comme pour le réseau interne, ce nom est requis, ou aucun port n'est marqué comme port externe.

État des paramètres de l'interface de gestion

Le graphique indique si la passerelle, les serveurs DNS, les serveurs NTP et les licences Smart sont configurés pour l'adresse de gestion et si ces paramètres fonctionnent correctement.

Le vert indique que la fonctionnalité est configurée et fonctionne correctement, le gris indique qu'elle n'est pas configurée ou ne fonctionne pas correctement. Par exemple, la zone DNS est grisée si les serveurs ne sont pas accessibles. Passez le curseur sur les éléments pour voir plus d'informations.

Si vous détectez des problèmes, corrigez-les comme suit :

- Port et passerelle de l'interface de gestion : sélectionnez **System Settings (Paramètres système)** > **Management Interface (Interface de gestion)**.
- Serveurs DNS : sélectionnez **System Settings (Paramètres système)** > **DNS Server**.
- Serveurs NTP : sélectionnez **System Settings (Paramètres système)** > **NTP**. Voir aussi Dépannage du protocole NTP, à la page 857.
- Licence Smart : cliquez sur le lien **View Configuration** (Afficher la configuration) dans le groupe Licence Smart.

Affichage de l'état des tâches du système

Les tâches système comprennent des actions qui se produisent sans votre participation directe, telles que la récupération et l'application de diverses mises à jour de base de données. Vous pouvez afficher une liste de ces tâches et leur état pour vérifier que ces tâches système sont effectuées avec succès.

La liste des tâches affiche l'état consolidé des tâches système et des tâches de déploiement. Le journal d'audit contient des informations plus détaillées et est accessible sous **Device (Périphérique)** > **Device Administration (Administration du périphérique)** > **Audit Log (Journal d'audit).** Par exemple, le journal d'audit affiche des événements distincts pour le début et la fin de la tâche, alors que la liste des tâches fusionne ces événements

en une seule entrée. En outre, l'entrée du journal d'audit d'un déploiement comprend des informations détaillées sur les modifications déployées.

Procédure

Étape 1 Cliquez sur le bouton **Task List** (Liste des tâches) dans le menu principal.



La liste des tâches s'ouvre, affichant l'état et les détails des tâches du système.

Étape 2 Évaluez l'état de la tâche.

Si vous détectez un problème persistant, vous devrez peut-être corriger la configuration du périphérique. Par exemple, un échec persistant à obtenir les mises à jour de la base de données peut indiquer qu'il n'y a pas de chemin d'accès à Internet pour l'adresse IP de gestion du périphérique. Vous devrez peut-être communiquer avec le centre d'assistance technique de Cisco (TAC) pour certains problèmes, comme indiqué dans les descriptions des tâches.

Vous pouvez effectuer les opérations suivantes avec la liste des tâches :

- Cliquez sur les boutons **Success** (Réussites) ou **Failures** (Échecs) pour filtrer la liste selon ces états.
- Cliquez sur l'icône de suppression () d'une tâche afin de la supprimer de la liste.
- Cliquez sur **Remove All Completed Tasks** (Supprimer toutes les tâches terminées) pour vider la liste de toutes les tâches qui ne sont pas en cours.

Utilisation de la console d'interface de ligne de commande pour surveiller et tester la configuration

Firewall Threat Defense Les périphériques comprennent une interface de ligne de commande (CLI) que vous pouvez utiliser pour la surveillance et le dépannage. Bien que vous puissiez ouvrir une session SSH pour obtenir l'accès à toutes les commandes du système, vous pouvez également ouvrir une console d'interface de ligne de commande dans le Gestionnaire de périphériques de pare-feu pour utiliser des commandes en lecture seule, telles que les diverses commandes **show** et **ping**, **traceroute**, et **packet-tracer**. Si vous disposez de privilèges d'administrateur, vous pouvez également accéder aux commandes **failover**, **reboot** et **shutdown**.

Vous pouvez laisser la console d'interface de ligne de commande ouverte pendant que vous vous déplacez d'une page à l'autre, configurez et déployez les fonctionnalités. Par exemple, après avoir déployé une nouvelle route statique, vous pouvez utiliser **ping** dans la console d'interface de ligne de commande pour vérifier que le réseau cible est accessible.

La console d'interface de ligne de commande utilise l'interface de ligne de commande de base Firepower Threat Defense. Vous ne pouvez pas accéder à l'interface de ligne de commande de diagnostic, au mode expert ou à l'interface de ligne de commande de FXOS (sur les modèles qui utilisent FXOS) à l'aide de la console d'interface de ligne de commande. Utilisez SSH si vous devez passer à ces autres modes de CLI.

Pour de plus amples renseignements, voir Référence de commande Cisco Firepower Threat Defense, https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.

Remarques :

- Bien que **ping** soit pris en charge dans la console CLI, la commande **ping system** n'est pas prise en charge.
- Le système peut traiter au maximum 2 commandes simultanées. Ainsi, si un autre utilisateur émet des commandes (par exemple, à l'aide de l'API REST), vous devrez peut-être attendre que d'autres commandes soient terminées avant d'entrer une commande. S'il s'agit d'un problème persistant, utilisez une session SSH au lieu de la console d'interface de ligne de commande.
- Les commandes renvoient des informations en fonction de la configuration déployée. Si vous apportez une modification de configuration dans Gestionnaire de périphériques de pare-feu, mais que vous ne la déployez pas, vous ne verrez pas les résultats de votre modification dans la sortie de commande. Par exemple, si vous créez une nouvelle route statique mais ne la déployez pas, cette route ne s'affichera pas dans la sortie **show route**.

Procédure

Étape 1 Cliquez sur le bouton **CLI Console** (Console CLI) dans le coin supérieur droit de la page Web.



Étape 2 Saisissez les commandes à l'invite et appuyez sur **Enter (Entrée)**.

Certaines commandes prennent plus de temps à produire une sortie que d'autres, veuillez patienter. Si vous recevez un message indiquant que l'exécution de la commande a expiré, veuillez réessayer. Vous obtiendrez également une erreur de délai d'expiration si vous entrez une commande qui nécessite des réponses interactives, comme **show perfstats**. Si le problème persiste, vous devrez peut-être utiliser un client SSH au lieu de la console d'interface de ligne de commande.

Voici quelques conseils sur la façon d'utiliser la fenêtre.

- Appuyez sur la touche **Tab** (Onglet) pour terminer automatiquement une commande après l'avoir partiellement saisie. De plus, Onglet répertorie les paramètres disponibles à ce stade de la commande. L'onglet fonctionne jusqu'à trois niveaux de mot-clé. Après trois niveaux, vous devez utiliser la référence de commande pour obtenir plus d'informations.
- Vous pouvez arrêter l'exécution de la commande en appuyant sur Ctrl+C.
- Pour déplacer la fenêtre, cliquez et maintenez n'importe où dans l'en-tête, puis faites glisser la fenêtre vers l'emplacement souhaité.
- Cliquez sur **Expand (Développer)** () ou **Collapse (Réduire)** () pour agrandir ou réduire la fenêtre.
- Cliquez sur le bouton **Undock Into Separate Window** (Détacher dans une fenêtre séparée) () pour dissocier la fenêtre de la page Web dans la fenêtre de son propre navigateur. Pour l'ancrer de nouveau, cliquez sur le bouton **Dock to Main Window** (Ancrer à la fenêtre principale) ().

- Cliquez et faites glisser pour surligner le texte, puis appuyez sur Ctrl+C pour copier le résultat dans le presse-papiers.
- Cliquez sur le bouton **Clear CLI (Effacer la CLI)** () pour effacer toute la sortie.
- Cliquez sur le bouton **Copy Last Output (Copier la dernière sortie)** () pour copier le résultat de la dernière commande que vous avez saisie dans le presse-papiers.

Étape 3 Lorsque vous avez terminé, fermez simplement la fenêtre de la console. N'utilisez pas la commande **exit**.

Bien que les informations d'authentification que vous utilisez pour vous connecter au Gestionnaire de périphériques de pare-feu valident votre accès à l'interface de ligne de commande, vous n'êtes jamais connecté à l'interface de ligne de commande lorsque vous utilisez la console.

Utilisation conjointe de Gestionnaire de périphériques de pare-feu et de l'API REST

Lorsque vous configurez le périphérique en mode gestion locale, vous pouvez le configurer à l'aide de FDM et de l'API REST Firepower Threat Defense. En fait, le Gestionnaire de périphériques de pare-feu utilise l'API REST pour configurer l'appareil.

Cependant, veuillez comprendre que l'API REST peut fournir des fonctionnalités supplémentaires que celles disponibles par l'intermédiaire du Gestionnaire de périphériques de pare-feu. Ainsi, pour une fonctionnalité donnée, vous pourrez peut-être configurer des paramètres à l'aide de l'API REST qui ne peuvent pas s'afficher lorsque vous affichez la configuration à l'aide de Gestionnaire de périphériques de pare-feu.

Si vous configurez un paramètre de fonctionnalité disponible dans l'API REST, mais pas dans Gestionnaire de périphériques de pare-feu, puis apportez une modification à la fonctionnalité globale (comme le VPN d'accès à distance) à l'aide de Gestionnaire de périphériques de pare-feu, ce paramètre peut être annulé. Le fait qu'un paramètre API uniquement soit conservé peut varier et, dans de nombreux cas, les modifications apportées par l'API aux paramètres non disponibles dans Gestionnaire de périphériques de pare-feu sont conservées par le biais des modifications Gestionnaire de périphériques de pare-feu. Pour une fonctionnalité donnée, vous devez vérifier si vos modifications sont conservées.

En général, vous devez éviter d'utiliser simultanément Gestionnaire de périphériques de pare-feu et l'API REST pour une fonctionnalité donnée. Au lieu de cela, choisissez une méthode ou une autre, fonctionnalité par fonctionnalité, pour configurer le périphérique.

Vous pouvez afficher et essayer les méthodes API à l'aide de l'explorateur API. Cliquez sur le bouton des autres options (⋮) et choisissez **API Explorer** (Explorateur d'interface de protocole d'application).

Exigences relatives aux ports de communication et à l'accès Internet

Les rubriques suivantes décrivent les ports qui doivent être ouverts sur le périphérique et les sites Internet auxquels l'accès est requis pour utiliser toutes les fonctionnalités disponibles sur le périphérique. Si vous

fonctionnez de manière limitée ou isolée, certains ou tous ces ports et sites Internet peuvent être bloqués pour répondre à vos besoins. Sinon, assurez-vous que ces ports et ces sites sont ouverts et accessibles.

Ports de communication utilisés par le périphérique

Les tableaux suivants répertorient les ports qui doivent être ouverts pour divers services. Utilisez des règles de contrôle d'accès pour vous assurer que l'accès à ces ports est ouvert sur les interfaces qui font face aux services ou qui font face aux utilisateurs qui devraient pouvoir accéder au périphérique à l'aide du protocole associé. Si vous n'utilisez pas de fonctionnalité, vous pouvez laisser ces ports fermés.

Tableau 2 : Ports entrants

Port entrant	Protocole/Fonctionnalité	Détails
TCP 22	SSH	Sécuriser les connexions distantes à l'interface de ligne de commande de l'appareil. **Remarque** Si vous utilisez la commande **copy** ou une autre commande qui effectue une communication externe, vous devez ouvrir ce port sortant. Par exemple, TCP/20, 21 si vous avez l'intention d'utiliser le protocole FTP.
UDP 161	SNMP	Autorisez l'accès aux MIB par interrogation SNMP.
TCP/443	HTTPS	Utilisé pour les services suivants : • Connexions de gestion à FDM. • API REST Cisco Firepower Threat Defense. • Connexions VPN SSL d'accès à distance. Si vous configurez un port personnalisé pour le VPN d'accès à distance, ouvrez ce port.
TCP/885	Portail captif	Communiquez avec une source d'identité de portail captif. Ceci est le port par défaut. Si vous configurez un autre port, ouvrez votre port personnalisé. Pour obtenir plus de renseignements, consultez Configurer les paramètres de la politique d'identité, à la page 479.
TCP/8989	Cisco Support Diagnostics (Diagnostics de l'assistance Cisco)	Accepte les demandes autorisées. Initie également les connexions sur ce port.

Tableau 3 : Ports sortants :

Port sortant :	Protocole/Fonctionnalité	Détails
UDP/53 (Si utilisé.) TCP/53	DNS	DNS. Normalement, UDP/53 est utilisé pour DNS. Mais si vous utilisez DNS sur TCP, ouvrez également TCP/53.
UDP/67 UDP/68	DHCP (protocole de configuration dynamique des hôtes)	DHCP.

Port sortant :	Protocole/Fonctionnalité	Détails
UDP/123	NTP;	Synchronisez l'heure.
UDP/162	SNMP	Envoyez des alertes SNMP à un serveur de déroutement distant.
TCP/389 TCP/636	LDAP, LDAPS	Communiquez avec un serveur LDAP pour l'authentification externe. Si vous configurez des ports personnalisés, ouvrez ces ports. Consultez Configuration des domaines d'identité AD, à la page 171.
TCP/443	HTTPS	Envoyer et recevoir des données d'Internet, par exemple pour télécharger des mises à jour de bases de données.
UDP/514	Syslog	Envoyez des messages de journal système à un serveur syslog distant.
UDP/1812 UDP/1813	RADIUS	Communiquez avec un serveur RADIUS pour l'authentification externe et la gestion comptable. Si vous configurez des ports personnalisés, ouvrez-les. Consultez Configurer les serveurs RADIUS, à la page 176.
UDP/8514	Cisco Secure Network Analytics Manager	Envoyez des messages de journalisation du système vers le nuage.
TCP/8989	Cisco Support Diagnostics (Diagnostics de l'assistance Cisco)	Transmet des informations et des statistiques d'utilisation. Accepte également les connexions sur ce port.

Ressources Internet consultées par le périphérique

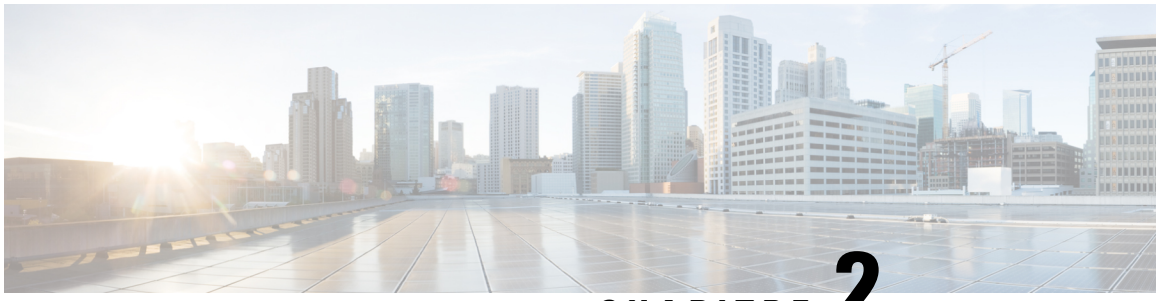
Les fonctionnalités suivantes doivent avoir accès aux ressources Internet associées pour fonctionner correctement. Le périphérique utilise les ports TCP/80 et TCP/443 selon les besoins.

Tableau 4 : Ressources Internet consultées par le périphérique

Caractéristiques	Motif	Haute disponibilité	Ressource
Offres groupées de certificats de l'autorité de certification (CA)	Demande de nouveaux certificats d'autorité de certification (CA) à une heure quotidienne définie par le système. L'offre groupée de l'autorité de certification locale contient des certificats pour accéder à plusieurs services Cisco. Cette fonctionnalité est configurée dans l'interface de ligne de commande à l'aide de la commande **configure cert-update auto-update**. Disponible dans les versions 7.0(5), 7.1(0.3), 7.2(4), 7.3 et ultérieures.	Chaque homologue télécharge ses propres certificats.	cisco.com/security/pki
Défense contre les programmes malveillants 1	Recherches Cisco AMP Cloud	Les deux homologues effectuent des recherches.	Adresses de serveur requises pour le bon fonctionnement de Cisco Secure Endpoint et le fonctionnement de Malware Analytics.
	Téléchargez les mises à jour de signatures pour la préclassification des fichiers et l'analyse des programmes malveillants locaux.	Les homologues actifs téléchargent et se synchronisent en mode veille.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	Envoyer des fichiers pour analyse dynamique. Requête de résultats d'analyse dynamique.	Les deux homologues soumettent ou interrogent des rapports d'analyse dynamique.	fmc.api.threatgrid.com fmc.api.threatgrid.eu fmc.api.threatgrid.ca fmc.api.threatgrid.com.au fmc.api.threatgrid.in
Renseignements de sécurité	Télécharger les flux de renseignements sur la sécurité	Les homologues actifs téléchargent et se synchronisent en mode veille.	intelligence.sourcefire.com

Caractéristiques	Motif	Haute disponibilité	Ressource
Filtrage d'URL	Télécharger des données de catégorie d'URL et de réputation. Interroger (rechercher) manuellement les données de catégorie d'URL et de réputation. Rechercher des URL non classées.	Les homologues actifs téléchargent et se synchronisent en mode veille.	URL : • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com Blocs IPv4 : • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 Blocs IPv6 : • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Propriété Smart Software Manager	Communiquez avec le Smart Software Manager.	L'homologue actif communique.	www.cisco.com
Cisco Success Network	Transmettez des informations et des statistiques d'utilisation.	L'homologue actif communique.	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
Cisco Support Diagnostics (Diagnostics de l'assistance Cisco)	Accepte les demandes autorisées et transmet les renseignements et les statistiques d'utilisation.	L'homologue actif communique.	api-sse.cisco.com:8989
Services en nuage généraux	—	—	api-sse.cisco.com
Intégration Cisco XDR	Configurer les périphériques pour envoyer des événements au Cisco Security Cloud.	L'homologue actif communique.	Guide d'intégration Cisco Secure Firewall Threat Defense et Cisco XDR.
Synchronisation de l'heure	Synchronisez l'heure dans votre déploiement. Non pris en charge avec un serveur mandataire.	Les deux homologues communiquent avec le serveur NTP.	Utilisateur configuré. Serveurs par défaut : • 0.sourcefire.pool.ntp.org • 1.sourcefire.pool.ntp.org • 2.sourcefire.pool.ntp.org

Caractéristiques	Motif	Haute disponibilité	Ressource
Règles d'intrusion	Télécharger les règles d'intrusion (SRU/LSP).	Les homologues actifs téléchargent et se synchronisent en mode veille.	talosintelligence.com
Base de données sur la vulnérabilité	Télécharger les mises à jour VDB.	Les homologues actifs téléchargent et se synchronisent en mode veille.	support.sourcefire.com
Base de données de géolocalisation	Télécharger les mises à jour GeoDB.	Les homologues actifs téléchargent et se synchronisent en mode veille.	support.sourcefire.com



CHAPITRE 2

Meilleures pratiques : scénarios d'utilisation pour Firewall Threat Defense

Les rubriques suivantes expliquent certaines tâches courantes que vous pourriez vouloir accomplir à l'aide de Firepower Threat Defense en utilisant FDM. Ces scénarios d'utilisation sont fondés sur l'hypothèse voulant que vous ayez terminé la configuration du périphérique avec l'assistant et que vous ayez conservé cette configuration initiale. Même si vous avez modifié la configuration initiale, vous devriez être en mesure d'utiliser ces exemples pour comprendre comment utiliser le produit.

- Comment configurer l'appareil en FDM, à la page 43
- Comment mieux comprendre le trafic de votre réseau, à la page 49
- Comment bloquer les menaces, à la page 56
- Comment bloquer les logiciels malveillants, à la page 61
- Comment mettre en œuvre une politique d'utilisation acceptable (filtrage d'URL), à la page 64
- Comment contrôler l'utilisation des applications, à la page 69
- Comment ajouter un sous-réseau, à la page 73
- Comment surveiller passivement le trafic sur un réseau, à la page 78
- Plus d'exemples, à la page 84

Comment configurer l'appareil en FDM

Après avoir terminé la configuration avec l'assistant, vous devriez avoir un périphérique qui fonctionne avec quelques règles de base en place :

- Interfaces interne et externe. Aucune autre interface de données n'est configurée.
- (Firepower 4100/9300) Les interfaces de données ne sont pas préconfigurées.
- (ISA 3000) Un groupe de ponts contient 2 interfaces internes et 2 interfaces externes. Vous devez définir manuellement l'adresse IP de BVI1 pour terminer votre configuration.
- (À l'exception de Firepower 4100/9300) Zones de sécurité pour les interfaces interne et externe.
- (À l'exception de Firepower 4100/9300) Une règle d'accès qui fait confiance au trafic interne vers externe. Pour l'ISA 3000, il existe des critères d'accès qui autorisent tout le trafic de l'intérieur vers l'extérieur et de l'extérieur vers l'intérieur.
- (À l'exception de Firepower 4100/9300 et ISA 3000) Une règle d'interface NAT qui traduit tout le trafic interne vers externe vers des ports uniques sur l'adresse IP de l'interface externe.

- (À l'exception de Firepower 4100/9300 et ISA 3000) Un serveur DHCP fonctionnant sur l'interface interne .

Les étapes suivantes donnent un aperçu des fonctionnalités supplémentaires que vous pourriez souhaiter configurer. Veuillez cliquer sur le bouton d'aide (**?**) dans une page pour obtenir des renseignements détaillés sur chaque étape.

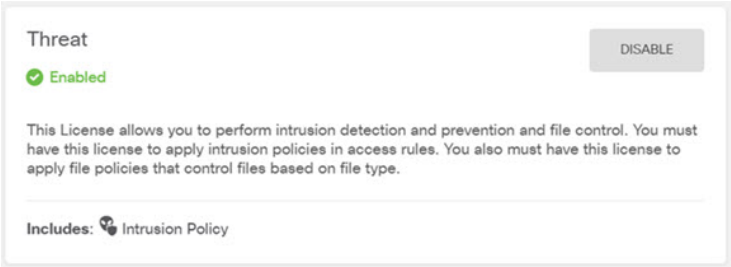
Procédure

Étape 1 Choisissez **Device (périphérique)**, cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Smart License** (Licence Smart).

Cliquez sur **Enable** (Activer) pour chacune des licences facultatives que vous souhaitez utiliser : Menace , Programme malveillant, URL. Si vous avez enregistré l'appareil pendant la configuration, vous pouvez également activer la licence VPN RA souhaitée. Lisez l'explication sur chaque licence si vous ne savez pas si vous en avez besoin.

Si vous n'êtes pas enregistré, vous pouvez le faire à partir de cette page. Cliquez sur **Register Device (enregistrer l'appareil)** et suivez les instructions. Veuillez vous inscrire avant l'expiration de la licence d'évaluation.

Par exemple, une licence (license Threat) activée devrait se présenter comme suit :



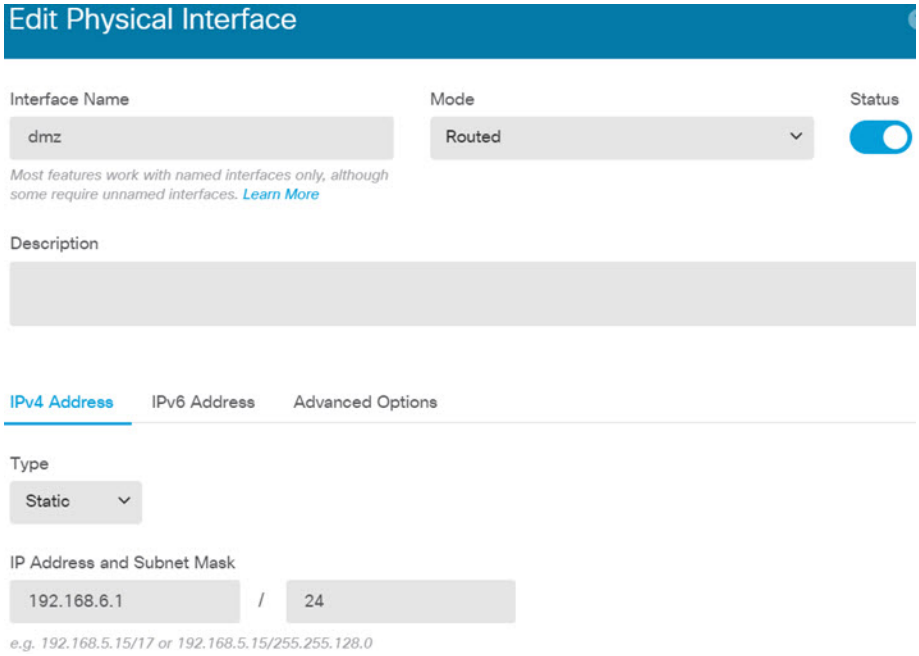
Étape 2 Si vous avez câblé d'autres interfaces, choisissez **Device (périphérique)**, puis cliquez sur le lien dans le résumé des **Interfaces**, puis cliquez sur le type d'interface pour afficher la liste des interfaces.

- Pour le Firepower 4100/9300, aucune interface de données n'est préconfigurée avec des noms, des adresses IP ou des zones de sécurité, vous devez donc activer et configurer les interfaces que vous souhaitez utiliser.
- Comme l'ISA 3000 sont préconfigurés avec un groupe de ponts contenant toutes les interfaces de données , il n'est pas nécessaire de configurer ces interfaces. Cependant, vous devez configurer manuellement une adresse IP pour le BVI. Si vous souhaitez dissocier le groupe de ponts, vous pouvez le modifier pour supprimer les interfaces que vous souhaitez traiter séparément. Vous pouvez ensuite configurer ces interfaces comme hôtes de réseaux distincts.

  Pour les autres modèles, vous pouvez créer un groupe de ponts pour les autres interfaces, ou configurer des réseaux distincts, ou une combinaison des deux.
- Pour le Firepower 1010, toutes les interfaces, à l'exception d'Ethernet1/1 (externe), sont des ports de commutation en mode d'accès affectés à VLAN1 (interne). Vous pouvez modifier les ports de commutation en ports de pare-feu; ajouter de nouvelles interfaces VLAN et y affecter des ports de commutation; ou configurer les ports de commutation en mode de ligne principale.

Cliquez sur l'icône de modification ( ) pour chaque interface afin de définir le mode, l'adresse IP et d'autres paramètres.

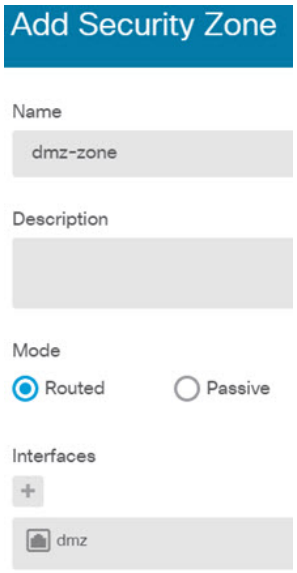
Dans l'exemple suivant, une interface est configurée pour être utilisée comme « zone démilitarisée » (DMZ), où vous placez des ressources accessibles au public, comme votre serveur Web. Lorsque vous avez terminé, cliquez sur **Save** (enregistrer).



Étape 3 Si vous avez configuré de nouvelles interfaces, sélectionnez **Objects** (objets), puis **Security Zones** (zones de sécurité) dans la table des matières.

Modifiez ou créez de nouvelles zones, selon le cas. Chaque interface doit appartenir à une zone, car vous configurez les politiques en fonction des zones de sécurité et non des interfaces. Vous ne pouvez pas placer les interfaces dans des zones lors de leur configuration. Par conséquent, vous devez toujours modifier les objets des zones après avoir créé de nouvelles interfaces ou modifié le but des interfaces existantes.

L'exemple suivant montre comment créer une nouvelle zone dmz pour l'interface dmz.

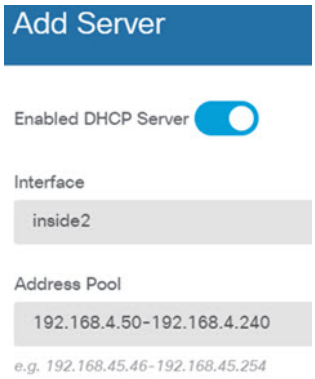


Étape 4 Si vous souhaitez que les clients internes utilisent le protocole DHCP pour obtenir une adresse IP du périphérique, sélectionnez **Device (périphérique)**, puis **System Settings (Paramètres système)** > **DHCP Server (Serveur DHCP)**. Sélectionnez l'onglet **DHCP Server** (Serveur DHCP).

Un serveur DHCP est déjà configuré pour l'interface interne, mais vous pouvez modifier l'ensemble des adresses ou même le supprimer. Si vous avez configuré d'autres interfaces internes, il est très courant de configurer un serveur DHCP pour ces interfaces. Cliquez sur **+** pour configurer le serveur et l'ensemble d'adresses pour chaque interface interne.

Vous pouvez également affiner la liste WINS et DNS fournie aux clients dans l'onglet **Configuration**.

L'exemple suivant montre comment configurer un serveur DHCP sur l'interface interne 2 avec l'ensemble d'adresses 192.168.4.50-192.168.4.240.



Étape 5 Choisissez **Device (périphérique)**, puis cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Routing** (Routage) et configurez une route par défaut.

La voie de routage par défaut s'oriente normalement vers le routeur ISP (ou en amont) qui se trouve à côté de l'interface externe. Une voie de routage IPv4 par défaut est configuré sur any-ipv4 (0.0.0.0/0), alors qu'un routage IPv6 par défaut est configuré sur any-ipv6 (:: 0/0). Créez le routage pour chaque version IP que vous utilisez. Si vous utilisez le protocole DHCP pour obtenir une adresse pour l'interface externe, vous avez peut-être déjà accès au routage par défaut dont vous avez besoin.

Les voies de routage que vous définissez sur cette page concernent uniquement les interfaces de données. Elles n'ont aucun impact sur l'interface de gestion. Définissez la passerelle de gestion sous **System Settings (Paramètres système)** > **Management Interface (Interface de gestion)**.

L'exemple suivant montre une voie de routage par défaut pour IPv4. Dans cet exemple, la passerelle isp-gateway est un objet réseau qui identifie l'adresse IP de la passerelle du fournisseur de services Internet (vous devez obtenir l'adresse de votre fournisseur de services Internet). Vous pouvez créer cet objet en cliquant sur **Create New Network** (créer un nouveau réseau) au bas du menu déroulant **Gateway** (passerelle).



Étape 6 Sélectionnez les politiques sous **Policies** et configurez les politiques de sécurité pour le réseau.

L'assistant de configuration de périphérique active le flux du trafic entre la zone interne et la zone externe ainsi que la NAT d'interface pour toutes les interfaces vers l'interface externe. Même si vous configurez de nouvelles interfaces, si vous les ajoutez à l'objet dans la zone interne, la règle de contrôle d'accès s'applique automatiquement à celles-ci.

Cependant, si vous avez plusieurs interfaces internes, vous avez besoin d'une règle de contrôle d'accès pour permettre la circulation du trafic d'une zone interne à une autre. Si vous ajoutez d'autres zones de sécurité, vous avez besoin de règles pour autoriser le trafic en provenance et à destination de ces zones. Il s'agit de vos modifications minimales.

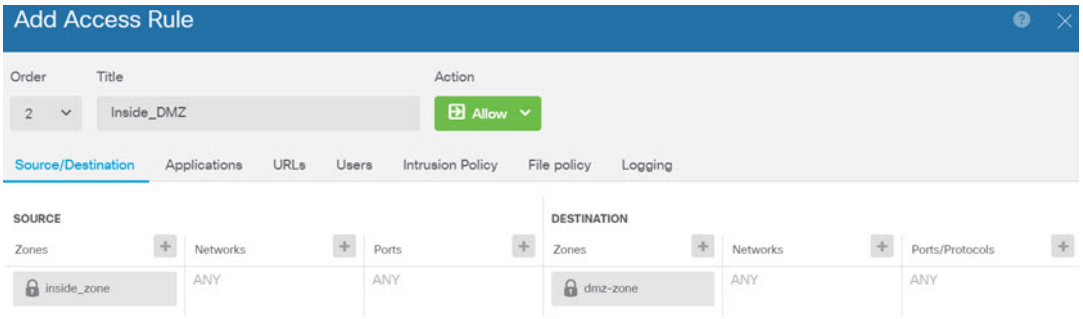
En outre, vous pouvez configurer d'autres politiques pour fournir des services supplémentaires et affiner la NAT et les règles d'accès afin d'obtenir les résultats requis par votre organisation. Vous pouvez configurer les politiques suivantes :

- **Déchiffrement SSL** : Si vous souhaitez inspecter les connexions chiffrées (comme HTTPS) pour détecter les intrusions, les logiciels malveillants, etc., vous devez déchiffrer les connexions. Utilisez la politique de déchiffrement SSL pour déterminer les connexions qui doivent être déchiffrées. Le système rechiffre la connexion après l'avoir inspectée.
- **Identité** : Si vous souhaitez corréler l'activité du réseau à des utilisateurs individuels ou contrôler l'accès au réseau en fonction de l'utilisateur ou de l'appartenance à un groupe d'utilisateurs, utilisez la politique d'identité pour déterminer l'utilisateur associé à une adresse IP source donnée.
- **Security Intelligence** (Renseignements sur la sécurité) : utilisez la politique sur les renseignements sur la sécurité pour supprimer rapidement les connexions en provenance des adresses IP ou des URL de la

liste de blocage ou vers celles-ci. En inscrivant sur la liste de blocage les mauvais sites connus, vous n'avez pas besoin de les prendre en compte dans votre politique de contrôle d'accès. Cisco fournit des flux régulièrement mis à jour d'adresses et d'adresses URL incorrectes afin que la liste de blocage issue des renseignements sur la sécurité se mette à jour de façon dynamique. En utilisant les flux, vous n'avez pas besoin de modifier la politique pour ajouter ou supprimer des éléments dans la liste de blocage.

- **NAT** (Network Address Translation, traduction d'adresses réseau) : utilisez la politique NAT pour convertir les adresses IP internes en adresses de routage externe.
- **Contrôle d'accès** : Utilisez la politique de contrôle d'accès pour déterminer les connexions autorisées sur le réseau. Vous pouvez procéder au filtrage selon la zone de sécurité, l'adresse IP, le protocole, le port, l'application, l'adresse URL, l'utilisateur ou le groupe d'utilisateurs. Vous pouvez aussi appliquer également des politiques en lien avec la prévention des intrusions et avec la présence de fichiers (logiciels malveillants) en utilisant des règles de contrôle d'accès. Utilisez cette politique pour mettre en œuvre le filtrage d'URL.
- **Intrusion** : Utilisez les politiques de prévention des intrusions pour rechercher les menaces connues. Bien que vous appliquiez des politiques de prévention des intrusions à l'aide de règles de contrôle d'accès, vous pouvez modifier lesdites politiques pour activer ou désactiver sélectivement des règles de prévention précises en lien avec les intrusions.

L'exemple suivant montre comment autoriser le trafic entre la zone interne et la zone dmz dans la politique de contrôle d'accès. Dans cet exemple, aucune option n'est définie sous les autres onglets, à l'exception de la journalisation (**Logging**), pour laquelle l'option **At End of Connection** (à la fin de la connexion) est sélectionnée.



Étape 7 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Comment mieux comprendre le trafic de votre réseau

Après avoir terminé la configuration initiale de l'appareil, vous disposerez d'une politique de contrôle d'accès qui permet à l'ensemble du trafic interne d'accéder à Internet ou à un autre réseau en amont, et d'une action par défaut pour bloquer tout autre trafic. Avant de créer des règles de contrôle d'accès supplémentaires, il peut être utile d'avoir accès à un aperçu du trafic qui se produit réellement sur votre réseau.

Vous pouvez utiliser les fonctionnalités de surveillance de Gestionnaire de périphériques de pare-feu pour analyser le trafic réseau. La création de rapports Gestionnaire de périphériques de pare-feu vous aide à répondre aux questions suivantes :

- À quoi sert mon réseau?
- Qui utilise le réseau le plus?
- Où vont mes utilisateurs?
- Quels appareils utilisent-ils?
- Quelles règles de contrôle d'accès (politiques) sont les plus touchées?

La règle d'accès initial peut donner un aperçu du trafic, y compris les politiques, les destinations et les zones de sécurité. Toutefois, pour obtenir des informations utilisateur, vous devez configurer une politique d'identité prévoyant une procédure d'authentification qui exige que les utilisateurs s'identifient eux-mêmes. Pour obtenir des informations sur les applications utilisées sur le réseau, vous devez effectuer quelques modifications supplémentaires.

La procédure suivante explique comment configurer l'appareil Firepower Threat Defense pour surveiller le trafic et donne un aperçu du processus de bout en bout de configuration et de surveillance des politiques.



Remarque Cette procédure ne donne pas un aperçu des catégories de sites Web et de la réputation des sites visités par les utilisateurs. Vous ne pouvez donc pas voir d'informations importantes dans le tableau de bord des catégories Web. Vous devez mettre en œuvre le filtrage d'URL par catégorie et activer la licence d'URL pour obtenir des données de catégorie et de réputation. Si vous souhaitez simplement obtenir ces informations, vous pouvez ajouter une nouvelle règle de contrôle d'accès qui autorise l'accès à une catégorie acceptable, comme Finance (finances) et en faire la première règle de la politique de contrôle d'accès. Pour en savoir plus sur la mise en œuvre du filtrage d'URL, consultez Comment mettre en œuvre une politique d'utilisation acceptable (filtrage d'URL), à la page 64.

Procédure

Étape 1 Pour mieux comprendre le comportement des utilisateurs, vous devez configurer une politique d'identité pour vous assurer que l'utilisateur associé à une connexion est identifié.

En activant la politique d'identité, vous pouvez recueillir des informations au sujet des utilisateurs du réseau et des ressources qu'ils utilisent. Ces informations sont disponibles dans le tableau de bord de contrôle des utilisateurs. Les informations sur l'utilisateur sont également disponibles pour les événements de connexion affichés dans le visualiseur d'événements.

Dans cet exemple, nous mettrons en œuvre l'authentification active pour obtenir de l'information sur l'identité de l'utilisateur. Grâce à une authentification active, l'appareil demande à l'utilisateur de fournir son nom d'utilisateur et son mot de passe. Les utilisateurs ne sont authentifiés que lorsqu'ils utilisent un navigateur Web pour les connexions HTTP.

Si un utilisateur ne parvient pas à s'authentifier, il peut néanmoins se connecter au Web. Toutefois, vous n'aurez pas accès à de l'information sur l'identité de l'utilisateur pour les connexions. Si vous le souhaitez, vous pouvez créer une règle de contrôle d'accès pour supprimer le trafic des utilisateurs ayant échoué à l'authentification.

a) Cliquez sur **Policies** (politiques) dans le menu principal, puis cliquez sur **Identity** (identité).

   La politique d'identité est initialement désactivée. Lorsque vous faites appel à l'authentification active, la politique d'identité utilise votre serveur Active Directory pour authentifier les utilisateurs et les associer à l'adresse IP du poste de travail qu'ils utilisent. Par la suite, le système identifiera le trafic pour cette adresse IP comme étant le trafic de l'utilisateur.

b) Cliquez sur **Enable Identity Policy** (activer la politique d'identité).

c) Cliquez sur le bouton **Create Identity Rule** (créer une règle d'identité) ou sur le bouton **+** pour créer la règle nécessitant une authentification active.

   Dans cet exemple, nous supposerons que vous souhaitez exiger l'authentification pour tout le monde.

d) Entrez un nom (**Name**) pour la règle, qui peut être tout ce que vous choisissez, par exemple, Require_Authentication.

e) Sous l'onglet **Source/Destination**, laissez les valeurs par défaut, qui s'appliquent à tout critère (Any).

   Vous pouvez appliquer à la politique les limites de votre choix pour établir un ensemble de trafic plus limité. Cependant, l'authentification active ne sera tentée que pour le trafic HTTP, donc c'est sans importance que le trafic non-HTTP corresponde (ou non) aux critères en lien avec la source/destination. Pour en savoir plus sur les propriétés de la politique d'identité, consultez Configurer les règles d'identité, à la page 481.

f) Sous **Action**, sélectionnez **Active Auth**.

   En supposant que vous n'ayez pas configuré les paramètres de politique d'identité, la boîte de dialogue Identity Policy Configuration (configuration de politique d'identité) s'ouvrira car il y a des paramètres non définis.

g) Configurez le portail captif et les paramètres de déchiffrement SSL requis pour l'authentification active.

   Lorsqu'une règle d'identité requiert une authentification active pour un utilisateur, l'utilisateur est redirigé vers le port du portail captif de l'interface par laquelle il est connecté, puis il est invité à s'authentifier. Le portail captif requiert des règles de déchiffrement SSL, que le système générera automatiquement, mais vous devez sélectionner le certificat à utiliser pour les règles de déchiffrement SSL.

   - **Server Certificate** (certificat de serveur) : Sélectionnez le certificat interne à présenter aux utilisateurs lors de l'authentification active. Vous pouvez sélectionner le certificat DefaultInternalCertificate autosigné prédéfini ou cliquer sur **Create New Internal Certificate** (créer un nouveau certificat interne) et télécharger un certificat déjà réputé fiable pour vos navigateurs.

     Les utilisateurs devront accepter le certificat si vous ne téléchargez pas un certificat déjà réputé fiable pour leurs navigateurs.

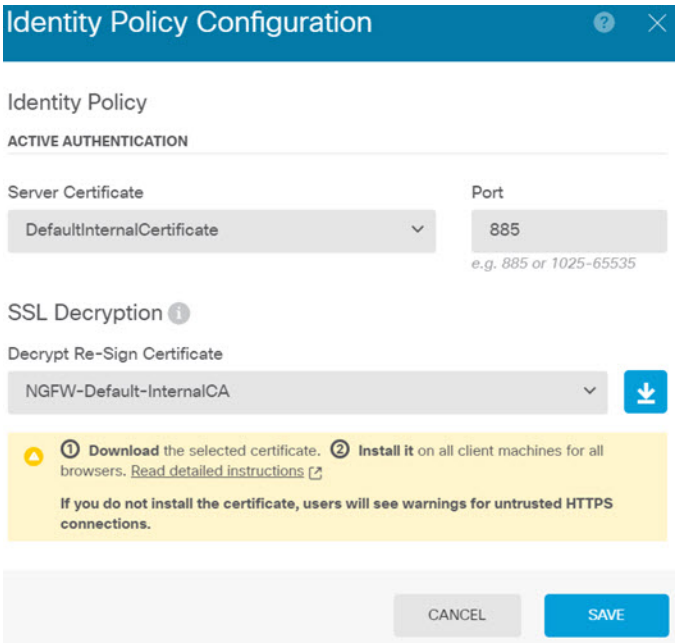
   - **Port** : le port du portail captif. La valeur par défaut est 885 (TCP). Si vous configurez un autre port, il doit être compris entre 1025 et 65535.

- **Decrypt Re-Sign Certificate** (déchiffrer le certificat resigné) : Sélectionnez le certificat d'autorité de certification interne à utiliser pour les règles qui mettent en application le déchiffrement avec les certificats resignés. Vous pouvez utiliser le certificat NGFW-Default-InternalCA prédéfini (par défaut) ou celui que vous avez créé ou téléchargé. Si le certificat n'existe pas encore, cliquez sur **Create Internal CA** (créer une autorité de certification interne) pour le créer. (Vous êtes invité à déchiffrer le certificat de re-signature seulement si vous n'avez pas encore activé la politique de déchiffrement SSL.)

  Si vous n'avez pas encore installé le certificat dans les navigateurs clients, cliquez sur le bouton de téléchargement ( ) pour en obtenir une copie. Consultez la documentation de chaque navigateur afin de savoir comment installer le certificat. Voir aussi Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature, à la page 469.

Exemple :

La boîte de dialogue Identity Policy Configuration (configuration de la politique d'identité) devrait maintenant ressembler à ce qui suit.



h) Cliquez sur **Save** pour enregistrer les paramètres d'authentification active.

L'onglet Active Authentication (authentification active) apparaît maintenant sous le paramètre Action.

i) Sous l'onglet **Authentification active** (authentification active), sélectionnez **HTTP Negotiate**.

Cela permet au navigateur et au serveur d'annuaire de négocier le protocole d'authentification le plus puissant, dans l'ordre, NTLM, puis HTTP de base.

Remarque
Pour les méthodes d'authentification HTTP de base, la page de réponse HTTP et NTLM, l'utilisateur est redirigé vers le portail captif en utilisant l'adresse IP de l'interface. Toutefois, pour la négociation HTTP, l'utilisateur est redirigé à l'aide du nom DNS complet *firewall-hostname.AD-domain-name*. Si vous souhaitez utiliser la négociation HTTP, vous devez également mettre à jour votre serveur DNS pour mapper ce nom aux adresses IP de toutes les interfaces internes pour lesquelles une authentification active est requise. Sinon, la redirection ne peut pas être terminée et les utilisateurs ne peuvent pas

s'authentifier. Si vous ne pouvez pas ou ne voulez pas mettre à jour le serveur DNS, sélectionnez l'une des autres méthodes d'authentification.

j) En ce qui concerne la source d'identité AD (**AD Identity Source**), cliquez sur **Create New Identity Realm** (créer un domaine d'identité).

Si vous avez déjà créé votre objet serveur de domaine, sélectionnez-le et ignorez les étapes de configuration du serveur.

Remplissez les champs suivants, puis cliquez sur **OK**.

- **Name** (nom) : Nom du domaine de répertoire.
- **Type** : Type de serveur d'annuaire. Active Directory est le seul type pris en charge et vous ne pouvez pas modifier ce champ.
- **Directory Username** (nom d'utilisateur), **Directory Password** (mot de passe d'annuaire) : nom d'utilisateur et mot de passe uniques pour un utilisateur disposant des droits appropriés sur les informations utilisateur que vous souhaitez récupérer. Pour Active Directory, l'utilisateur n'a pas besoin d'avoir des privilèges élevés. Vous pouvez préciser n'importe quel utilisateur dans le domaine. Le nom d'utilisateur doit être complet; par exemple, Administrateur@exemple.com (pas simplement Administrateur).

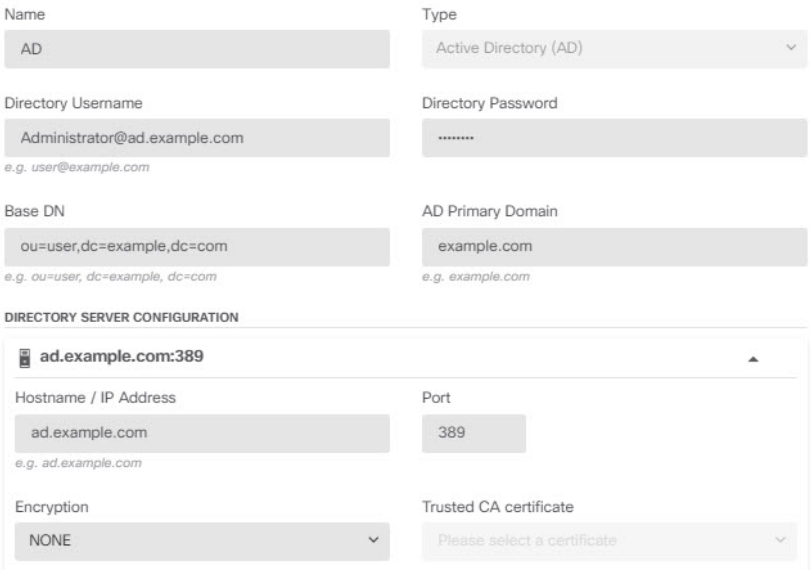
  Remarque
  Le système génère ldap-login-dn et ldap-login-password à partir de ces informations. Par exemple, Administrateur@exemple.com se traduit par cn=adminisntrator,cn=users,dc=example,dc=com. Notez que cn=users fait toujours partie de cette traduction; vous devez donc configurer l'utilisateur que vous précisez ici sous le nom usuel du dossier « users ».

- **Base DN** (base DN) : L'arborescence pour faire des recherches ou requêtes d'informations sur les utilisateurs et les groupes, c'est-à-dire le parent commun des utilisateurs et des groupes. Par exemple, dc=example,dc=com. Pour en savoir plus sur la recherche du DN de base, consultez Détermination du DN de base du répertoire, à la page 170.
- **AD Primary Domain** (domaine principal AD) : le nom de domaine complet d'Active Directory que le périphérique doit joindre.' Par exemple, exemple.com.
- **Hostname/IP Address** (nom d'hôte/adresse IP) : le nom d'hôte ou l'adresse IP du serveur d'annuaire. Si vous utilisez une connexion chiffrée avec le serveur, vous devez saisir le nom de domaine complet, et non l'adresse IP.
- **Port** : le numéro de port utilisé pour les communications avec le serveur. La valeur par défaut est 389. Utilisez le port 636 si vous sélectionnez LDAPS comme méthode de chiffrement.
- **Encryption** (chiffrement) : Pour utiliser une connexion chiffrée pour le téléchargement des informations sur les utilisateurs et les groupes, sélectionnez la méthode souhaitée, **STARTTLS** ou **LDAPS**. La valeur par défaut est **None** (aucun), ce qui signifie que les informations relatives aux utilisateurs et aux groupes sont téléchargées en texte en clair.
  - **STARTTLS** négocie la méthode de chiffrement et utilise la méthode la plus efficace prise en charge par le serveur d'annuaire. Utilisez le port 389. Cette option n'est pas prise en charge si vous utilisez le domaine pour le VPN d'accès à distance.
  - **LDAPS** nécessite LDAP sur SSL. Utilisez le port 636.

- **Trusted CA Certificate** (certificat CA de confiance) : Si vous sélectionnez une méthode de chiffrement, téléchargez un certificat d'autorité de certification (CA) pour activer une connexion de confiance entre le système et le serveur d'annuaire. Si vous utilisez un certificat pour vous authentifier, le nom du serveur dans le certificat doit correspondre au nom d'hôte ou à l'adresse IP du serveur. Par exemple, si vous utilisez 10.10.10.250 comme adresse IP mais ad.exemple.com dans le certificat, la connexion échouera.

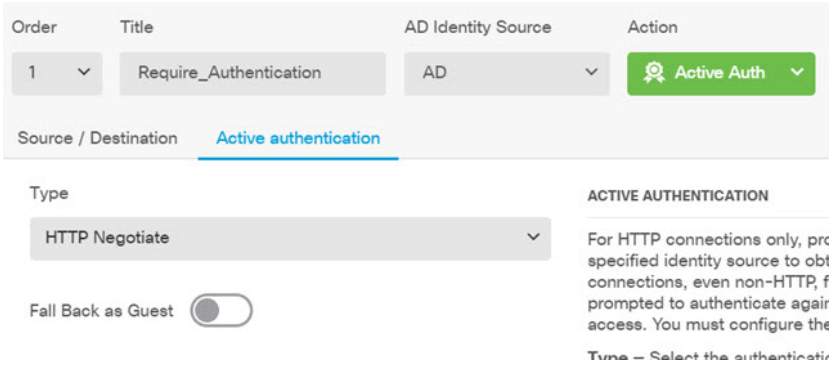
Exemple :

Par exemple, l'image suivante montre comment créer une connexion non chiffrée pour le serveur ad.exemple.com. Le domaine principal est exemple.com et le nom d'utilisateur du répertoire est Administrateur@ad.exemple.com. Toutes les informations relatives aux utilisateurs et aux groupes se trouvent sous le nom distinctif (DN) ou=user,dc=example,dc=com.



k) Pour la **source d'identité AD**, sélectionnez l'objet que vous venez de créer.

La règle devrait ressembler à ce qui suit.



l) Cliquez sur **OK** pour ajouter la règle.

Si vous regardez dans le coin supérieur droit de la fenêtre, vous pouvez voir que le bouton d'icône **Deploy** (déployer) a maintenant un point, ce qui indique qu'il y a des changements non déployés. Apporter des modifications à l'interface utilisateur n'est pas suffisant pour configurer les modifications

sur l'appareil. Vous devez déployer les modifications. Ainsi, vous pouvez apporter un ensemble de modifications connexes avant de les déployer, afin d'éviter les problèmes susceptibles de découler de l'exécution sur le périphérique d'un ensemble de modifications partiellement configuré. Vous déploierez les modifications plus tard dans cette procédure.

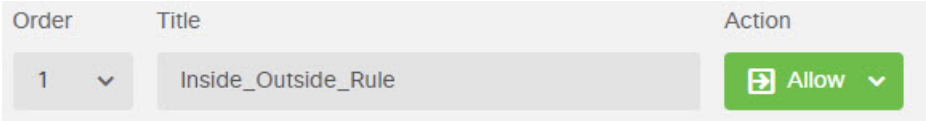


Étape 2 Modifiez l'action de la règle de contrôle d'accès Inside_Outside_Rule afin de l'autoriser (**Allow**).

La règle d'accès Inside_Outside_Rule est créée en tant que règle de confiance. Cependant, le trafic considéré comme digne de confiance n'est pas inspecté, de sorte que le système ne peut pas connaître certaines de ses caractéristiques, comme l'application, lorsque les critères de correspondance du trafic n'incluent pas l'application ou d'autres conditions que la zone, l'adresse IP et le port. Si vous modifiez la règle pour autoriser le trafic plutôt que de lui accorder votre confiance, le système inspectera entièrement le trafic.

Remarque
(ISA 3000.) Vous pouvez également envisager de modifier les paramètres de Outside_Inside_Rule, Inside_Inside_Rule et Outside_Outside_Rule de « Trust » (faire confiance) à « Allow » (autoriser).

a) Cliquez sur **Access Control** (contrôle d'accès) dans la page des politiques (**Policies**).
b) Passez la souris sur la cellule **Actions** sur le côté droit de la rangée Inside_Outside_Rule pour exposer les icônes de modification et de suppression, puis cliquez sur l'icône de modification ( ) pour ouvrir la règle.
c) Sélectionnez **Allow** (autoriser) sous **Action**.

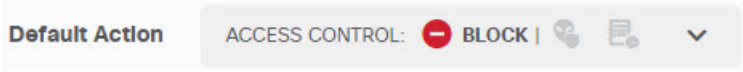


d) Cliquez sur **OK** pour enregistrer la modification

Étape 3 Activez la journalisation de l'action par défaut de la politique de contrôle d'accès.

Les tableaux de bord contiennent des informations sur les connexions uniquement dans les cas où la connexion correspond à une règle de contrôle d'accès qui permet la journalisation des connexions. La règle Inside_Outside_Rule permet la journalisation, mais l'action par défaut désactive la journalisation. Ainsi, les tableaux de bord affichent uniquement des informations sur la règle Inside_Outside_Rule et ne reflètent pas les connexions qui ne correspondent à aucune règle.

a) Cliquez n'importe où dans l'action par défaut au bas de la page de politique de contrôle d'accès.



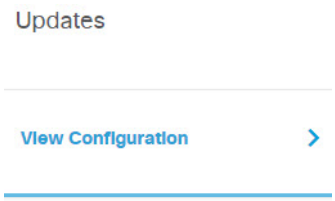
b) Sélectionnez la journalisation au début et à la fin de la connexion (**Select Log Action** > **At Beginning and End of Connection**).
c) Cliquez sur **OK**.

Étape 4 Définissez un calendrier de mises à jour pour la base de données sur les vulnérabilités (VDB).

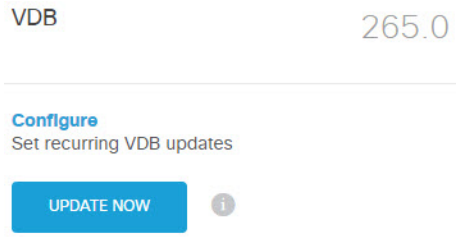
Cisco diffuse régulièrement des mises à jour de la VDB, qui comprend les détecteurs d'applications pouvant reconnaître l'application utilisée dans une connexion. Vous devez mettre à jour la VDB régulièrement. Vous pouvez soit télécharger manuellement les mises à jour, soit configurer un calendrier de mises à jour régulières.

La procédure suivante montre comment configurer un calendrier. Par défaut, les mises à jour de la base de données sur les vulnérabilités sont désactivées. Vous devez donc les activer pour mettre à jour la VDB.

a) Cliquez sur **Device (périphérique)**.
b) Cliquez sur **View Configuration** dans le groupe Updates (mises à jour).



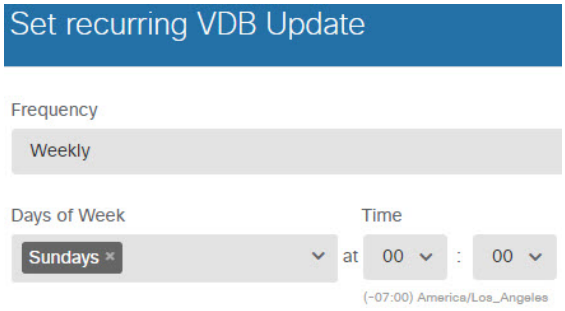
c) Cliquez sur **Configure** (configurer) dans le groupe VDB.



d) Définir le calendrier de mises à jour.

Choisissez une heure et une fréquence qui ne perturberont pas votre réseau. Il faut comprendre que le système effectuera un déploiement automatique après le téléchargement de la mise à jour. C'est nécessaire pour activer les nouveaux détecteurs. Ainsi, toutes les modifications de configuration que vous avez apportées et enregistrées, mais que vous n'avez pas encore déployées, seront également déployées.

Par exemple, voici l'horaire de la mise à jour de la VDB une fois par semaine, le dimanche, à minuit.



e) Cliquez sur **Save** (Enregistrer).

Étape 5 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Prochaine étape

À ce stade, les tableaux de bord et les événements de surveillance devraient commencer à afficher des informations sur les utilisateurs et les applications. Vous pouvez évaluer ces informations pour rechercher des tendances indésirables et élaborer de nouvelles règles d'accès pour limiter les utilisations inacceptables.

Si vous souhaitez commencer à recueillir des informations sur les intrusions et les logiciels malveillants, vous devez activer les politiques de prévention des intrusions et des politiques de fichiers sur l'une ou plusieurs des règles d'accès. Vous devez également activer les licences pour ces fonctionnalités.

Si vous souhaitez commencer à recueillir des informations sur les catégories d'URL, vous devez mettre en œuvre le filtrage d'URL.

Comment bloquer les menaces

Vous pouvez mettre en œuvre le filtrage IPS (Intrusion Prevention System) de nouvelle génération en ajoutant des politiques de prévention des intrusions à vos règles de contrôle d'accès. Les politiques de prévention des intrusions analysent le trafic réseau et comparent le contenu du trafic aux menaces connues. Si une connexion correspond à une menace que vous surveillez, le système la coupe, empêchant ainsi l'attaque.

Tous les autres traitements de trafic ont lieu avant que le trafic réseau ne fasse l'objet d'un examen pour détecter les intrusions. En associant une politique de prévention des intrusions à une règle de contrôle d'accès, vous informez le système qu'avant que soit transmis le trafic correspondant aux conditions de la règle de contrôle d'accès, vous souhaitez inspecter le trafic au moyen d'une politique de prévention des intrusions.

Vous pouvez configurer des politiques de prévention des intrusions uniquement sur des règles qui autorisent (**allow**) le trafic. Aucune inspection n'est effectuée sur les règles définies pour attribuer la confiance (**trust**) à un trafic ou le bloquer (**block**). En outre, vous pouvez configurer une politique de prévention des intrusions dans le cadre de l'action par défaut si l'action par défaut est **allow** (autoriser).

Les politiques d'intrusion sont conçues par le Cisco Talos Intelligence Group (Talos), qui définit les états des règles d'intrusion et de préprocesseur et les paramètres avancés. Vous pouvez créer vos propres politiques personnalisées en fonction des politiques Talos si vous utilisez Snort 3 comme moteur d'inspection.

En plus d'inspecter le trafic que vous autorisez afin de détecter d'éventuelles intrusions, vous pouvez utiliser la politique de renseignement de sécurité pour bloquer de manière préventive tout le trafic en provenance ou à destination d'adresses IP ou d'adresses URL connues comme mauvaises.

Procédure

Étape 1 Si vous ne l'avez pas encore fait, activez la licence Menace .

Vous devez activer la licence Menace pour utiliser les politiques de prévention des intrusions et les renseignements sur la sécurité. Si vous utilisez actuellement la licence d'évaluation, vous activez une version d'évaluation de la licence. Si vous avez enregistré l'appareil, vous devez acheter la licence requise et l'ajouter à votre compte Smart Software Manager sur Cisco.com.

a) Cliquez sur **Device (périphérique)**.
b) Cliquez sur **View Configuration** dans le groupe des licences Smart.



c) Cliquez sur **Enable** (activer) dans le groupe **Menace** .

Le système enregistre la licence avec votre compte ou active la licence d'évaluation, selon le cas. Le groupe doit indiquer que la licence est activée, et le bouton indique Disable (désactivé).



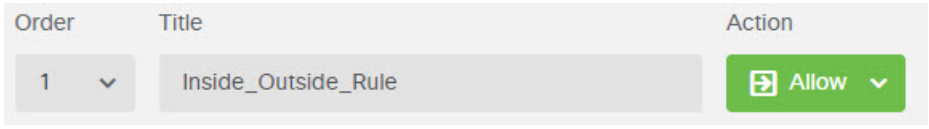
Étape 2 Sélectionnez une politique de prévention des intrusions pour l'une ou plusieurs des règles d'accès.

Déterminez les règles qui couvrent le trafic qui doit faire l'objet de l'analyse pour la recherche de menaces. Pour cet exemple, nous allons ajouter l'inspection en lien avec la prévention des intrusions à la règle Inside_Outside_Rule.

a) Cliquez sur **Policies** (politiques) dans le menu principal.

Assurez-vous que la politique de contrôle d'accès (**Access Control**) est affichée.

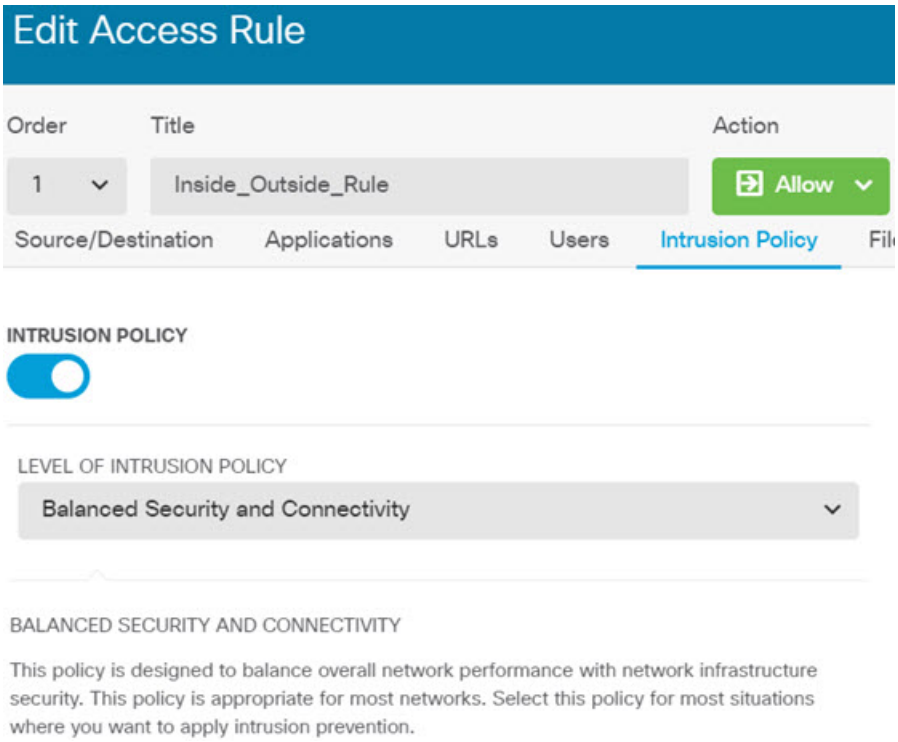
b) Passez la souris sur la cellule **Actions** sur le côté droit de la rangée Inside_Outside_Rule pour exposer les icônes de modification et de suppression, puis cliquez sur l'icône de modification ( ) pour ouvrir la règle.
c) Si vous ne l'avez pas encore fait, sélectionnez **Allow**(autoriser) pour l'action (**Action**).



d) Cliquez sur l'onglet **Intrusion Policy** (politique de prévention des intrusions).
e) Cliquez sur le bouton **Intrusion Policy** (politique de prévention des intrusions) pour l'activer, puis sélectionnez la politique.

La politique **Balanced Security and Connectivity**(sécurité et connectivité équilibrées) convient à la plupart des réseaux. Elle offre une bonne protection contre les intrusions sans être trop agressive, ce qui peut entraîner l'abandon d'un trafic que vous pourriez ne pas vouloir supprimer. Si vous déterminez que vous perdez trop de trafic, vous pouvez simplifier l'inspection en lien avec la prévention des intrusions en sélectionnant la politique **Connectivity over Security** (connectivité avant sécurité).

Si vous avez besoin de plus d'agressivité en matière de sécurité, essayez la politique **Security over Connectivity** (sécurité avant connectivité). La politique de détection maximale (**Maximum Detection**) accorde encore plus d'importance à la sécurité de l'infrastructure réseau, ce qui peut avoir un impact opérationnel encore plus important.



f) Cliquez sur **OK** pour enregistrer la modification

Étape 3 (Facultatif) Rendez-vous sur **Policies (politiques)** > **Intrusion**, cliquez sur l'icône en forme de roue et configurez un serveur syslog pour la politique de prévention des intrusions.

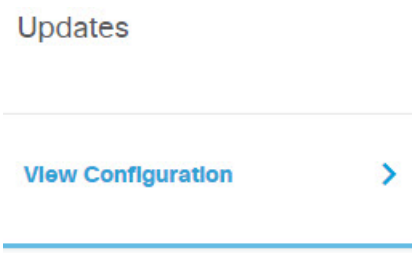
Les incidents d'intrusion n'utilisent pas le serveur syslog configuré pour la règle de contrôle d'accès.

Étape 4 Définir un calendrier de mise à jour pour la base de données des règles de prévention des intrusions.

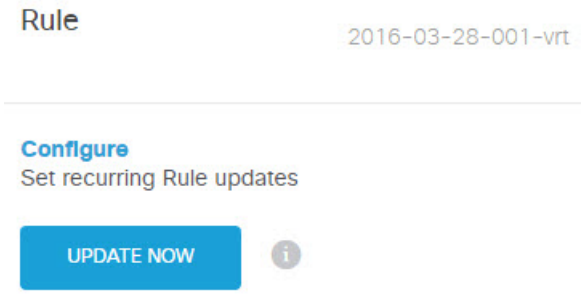
Cisco publie régulièrement des mises à jour de la base de données des règles de prévention des intrusions, qui est utilisée par les politiques d'intrusion pour déterminer si les connexions doivent être abandonnées. Vous devez mettre à jour la base de données des règles régulièrement. Vous pouvez soit télécharger manuellement les mises à jour, soit configurer un calendrier de mises à jour régulières. La procédure suivante montre comment configurer un calendrier. Par défaut, les mises à jour de la base de données sont désactivées. Vous devez donc prendre des mesures pour obtenir des règles mises à jour.

a) Cliquez sur **Device (périphérique)**.

b) Cliquez sur **View Configuration** dans le groupe Updates (mises à jour).



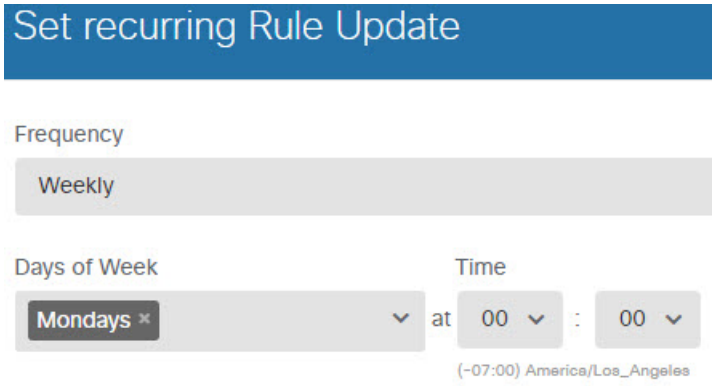
c) Cliquez sur **Configure** (configurer) dans le groupe des règles (Rule).



d) Définir le calendrier de mises à jour.

Choisissez une heure et une fréquence qui ne perturberont pas votre réseau. Il faut comprendre que le système effectuera un déploiement automatique après le téléchargement de la mise à jour. C'est nécessaire pour activer les nouvelles règles. Ainsi, toutes les modifications de configuration que vous avez apportées et enregistrées, mais que vous n'avez pas encore déployées, seront également déployées.

Par exemple, voici l'horaire de la mise à jour de la base de données sur les règles une fois par semaine, le lundi, à minuit.



e) Cliquez sur **Save** (Enregistrer).

Étape 5 Configurez la politique de renseignement de sécurité pour supprimer de manière préventive les connexions avec des sites et des hôtes connus comme mauvais.

En utilisant les renseignements de sécurité pour bloquer les connexions avec les hôtes ou les sites qui sont connus pour être des menaces, vous évitez à votre système le temps nécessaire pour effectuer une inspection approfondie des paquets afin de repérer les menaces dans chaque connexion. Les renseignements de sécurité permettent de bloquer rapidement le trafic indésirable, laissant plus de temps au système pour gérer le trafic important pour vous.

a) Cliquez sur **Device** (périphérique), puis sur **View Configuration** (afficher la configuration) dans le groupe **Updates** (mises à jour).
b) Cliquez sur **Update Now** (mettre à jour maintenant) dans le groupe Security Intelligence Feeds (flux de renseignements de sécurité).
c) Cliquez également sur **Configure** (configurer) et définissez une mise à jour périodique pour les flux. La valeur par défaut, **Hourly** (mise à jour toutes les heures), convient à la plupart des réseaux, mais vous pouvez réduire la fréquence si nécessaire.
d) Cliquez sur **Policies** (politiques), puis sur la politique **Security Intelligence** (renseignements de sécurité).
e) Cliquez sur **Enable Security Intelligence** si vous n'avez pas encore activé la politique.

f) Dans l'onglet **Network** (réseau), cliquez sur **+** dans la liste bloquer/abandonner (block/drop), puis sélectionnez tous les flux dans l'onglet **Network Feeds** (flux réseau). Vous pouvez cliquer sur le bouton **i** à côté d'un flux pour lire sa description.

Si vous voyez un message indiquant qu'il n'y a pas encore de flux, réessayez plus tard. Le téléchargement des flux n'est pas encore terminé. Si ce problème persiste, assurez-vous qu'il y a un chemin entre l'adresse IP de gestion et Internet.

g) Cliquez sur **OK** pour ajouter les flux sélectionnés.

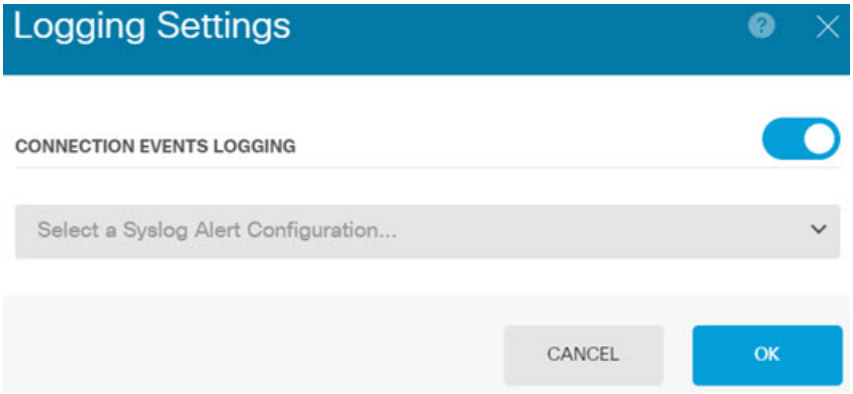
Si vous connaissez d'autres adresses IP incorrectes, vous pouvez cliquer sur **+** > **Network Objects** et ajouter les objets qui contiennent les adresses. Vous pouvez cliquer sur **Create New Network Object** (créer un nouvel objet réseau) au bas de la liste pour les ajouter immédiatement.

h) Cliquez sur l'onglet **URL**, puis sur **+** > **URL Feeds** dans la liste block/drop, enfin, sélectionnez tous les flux URL. Cliquez sur **OK** pour les ajouter à la liste.

Comme pour la liste de réseaux, vous pouvez ajouter vos propres objets URL à la liste pour bloquer d'autres sites qui ne sont pas dans les flux. Cliquez sur **+** > **URL Objects (objets URL)**. Vous pouvez ajouter de nouveaux objets en cliquant sur **Create New URL Object** (créer un nouvel objet URL) à la fin de la liste.

i) Cliquez sur l'icône en forme de roue et activez la journalisation des événements de connexion (**Connection Events Logging**) pour permettre à la politique de générer des événements de renseignements de sécurité pour les connexions correspondantes. Cliquez sur **OK** pour enregistrer les modifications.

Si vous n'activez pas la journalisation des connexions, vous n'aurez aucune donnée à utiliser pour déterminer si la politique répond aux attentes. Si un serveur syslog externe est défini, vous pouvez le sélectionner maintenant afin que les événements soient également envoyés à ce serveur.



j) Au besoin, vous pouvez ajouter des objets réseau ou URL à la liste **Do Not Block** (ne pas bloquer) dans chaque onglet pour créer des exceptions à la liste de contacts bloqués.

Les listes **Do Not Block** ne sont pas vraiment des listes encadrant les autorisations. Ce sont plutôt des listes d'exceptions. Si une adresse ou une URL dans la liste d'exceptions apparaît également dans la liste des contacts bloqués, la connexion pour l'adresse ou l'URL est transmise à la politique de contrôle d'accès. De cette façon, vous pouvez bloquer un flux, mais si vous constatez plus tard qu'une adresse ou un site souhaitable est bloqué, vous pouvez utiliser la liste des exceptions pour remplacer ce blocage sans devoir supprimer complètement le flux. Gardez à l'esprit que ces connexions sont ensuite évaluées par le contrôle d'accès et, si elles sont configurées, par des politiques de prévention des intrusions. Ainsi, si des connexions contiennent des menaces, elles peuvent être identifiées et bloquées lors d'une inspection de prévention des intrusions.

Consultez le tableau de bord de règles d'accès et de règles SI, ainsi que l'écran des renseignements sur la sécurité (Security Intelligence) dans le visualiseur d'événements, pour déterminer le trafic qui est réellement abandonné par la politique et établir si vous devez ajouter des adresses ou des URL aux listes **Do Not Block**.

Étape 6 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Prochaine étape

À ce stade, les tableaux de bord et les événements de surveillance devraient commencer à afficher des informations sur les auteurs des attaques, les cibles et les menaces, si des intrusions sont détectées. Vous pouvez évaluer ces informations pour déterminer si votre réseau a besoin de précautions de sécurité renforcées, ou si vous devez réduire le niveau des politiques de prévention des intrusions que vous utilisez.

Pour les renseignements de sécurité, vous pouvez voir les occurrences des politiques sur le tableau de bord des règles d'accès et de SI. Vous pouvez également voir les événements en lien avec les renseignement de sécurité dans le visualiseur d'événements. Les blocs fondés sur les renseignements de sécurité ne sont pas reflétés dans les renseignements sur les menaces d'intrusion, car le trafic est bloqué avant de pouvoir être inspecté.

Comment bloquer les logiciels malveillants

Les utilisateurs risquent continuellement d'obtenir des logiciels malveillants, ou *maliciels*, à partir de sites Internet ou d'autres méthodes de communication, comme le courrier électronique. Même des sites Web de confiance peuvent être piratés pour transmettre des logiciels malveillants à des utilisateurs peu méfiants. Les pages Web peuvent contenir des objets provenant de différentes sources. Ces objets peuvent inclure des images, des exécutables, du Javascript, des publicités, etc. Les sites Web compromis comprennent souvent des objets hébergés sur des sources externes. Une véritable solution de sécurité signifie regarder chaque objet individuellement, pas seulement la demande initiale.

Utilisez des politiques de fichiers pour détecter les programmes malveillants à l'aide du logiciel de défense contre les programmes malveillants. Vous pouvez également utiliser les politiques de fichiers pour effectuer le contrôle de fichier, ce qui permet de contrôler tous les fichiers d'un type spécifique, qu'ils contiennent ou non des logiciels malveillants.

Le logiciel de défense contre les programmes malveillants utilise Cisco AMP Cloud pour récupérer les dispositions relatives aux éventuels programmes malveillants détectés dans le trafic réseau. L'interface de gestion doit disposer d'un chemin vers Internet pour atteindre Cisco AMP Cloud et effectuer des recherches de programmes malveillants. Lorsque l'appareil détecte un fichier admissible, il utilise la valeur de hachage SHA-256 du fichier pour demander la Cisco AMP Cloud disposition du fichier. Voici les dispositions possibles

d'un fichier : inoffensif (**clean**), malveillant (**malware**) ou inconnu (**unknown**; aucun verdict clair). Si le Cisco AMP Cloud n'est pas accessible, la disposition est **inconnue**.

En associant une politique de fichiers à une règle de contrôle d'accès, vous informez le système qu'avant de transmettre le trafic correspondant aux conditions de la règle de contrôle d'accès, vous devez d'abord inspecter tous les fichiers de la connexion.

Vous pouvez configurer des politiques de fichiers uniquement sur des règles qui autorisent (**allow**) le trafic. Aucune inspection n'est effectuée sur les règles définies pour attribuer la confiance (**trust**) à un trafic ou le bloquer (**block**).

Procédure

Étape 1 Si vous ne l'avez pas encore fait, activez les licences Programme malveillant et Menace .

Vous devez activer la licence Programme malveillant pour utiliser les politiques de fichiers en plus de la licence Menace , qui est requise pour les politiques de détection des intrusions. Si vous utilisez actuellement la licence d'évaluation, vous activez une version d'évaluation des licences. Si vous avez enregistré l'appareil, vous devez acheter les licences requises et les ajouter à votre compte Smart Software Manager sur Cisco.com.

a) Cliquez sur **Device (périphérique)**.
b) Cliquez sur **View Configuration** dans le groupe des licences Smart.



c) Cliquez sur **Enable** (activer) dans le groupe **Programme malveillant** et, si ce n'est déjà fait, dans le groupe **Menace** .

Le système enregistre la licence avec votre compte ou active la licence d'évaluation, selon le cas. Le groupe doit indiquer que la licence est activée, et le bouton indique Disable (désactivé).



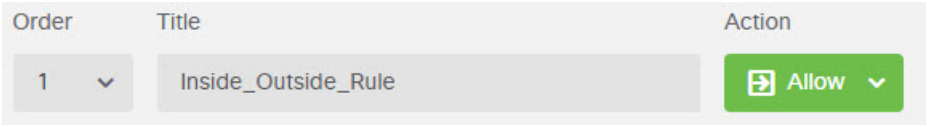
Étape 2 Sélectionnez une politique de fichiers pour l'une ou plusieurs des règles d'accès.

Déterminez les règles qui couvrent le trafic qui doit faire l'objet de l'analyse pour la recherche de logiciels malveillants. Pour cet exemple, nous allons ajouter l'inspection des fichiers à la règle Inside_Outside_Rule.

a) Cliquez sur **Policies** (politiques) dans le menu principal.

Assurez-vous que la politique de contrôle d'accès (**Access Control**) est affichée.

b) Passez la souris sur la cellule **Actions** sur le côté droit de la rangée Inside_Outside_Rule pour exposer les icônes de modification et de suppression, puis cliquez sur l'icône de modification ( ) pour ouvrir la règle.
c) Si vous ne l'avez pas encore fait, sélectionnez **Allow**(autoriser) pour l'action (**Action**).



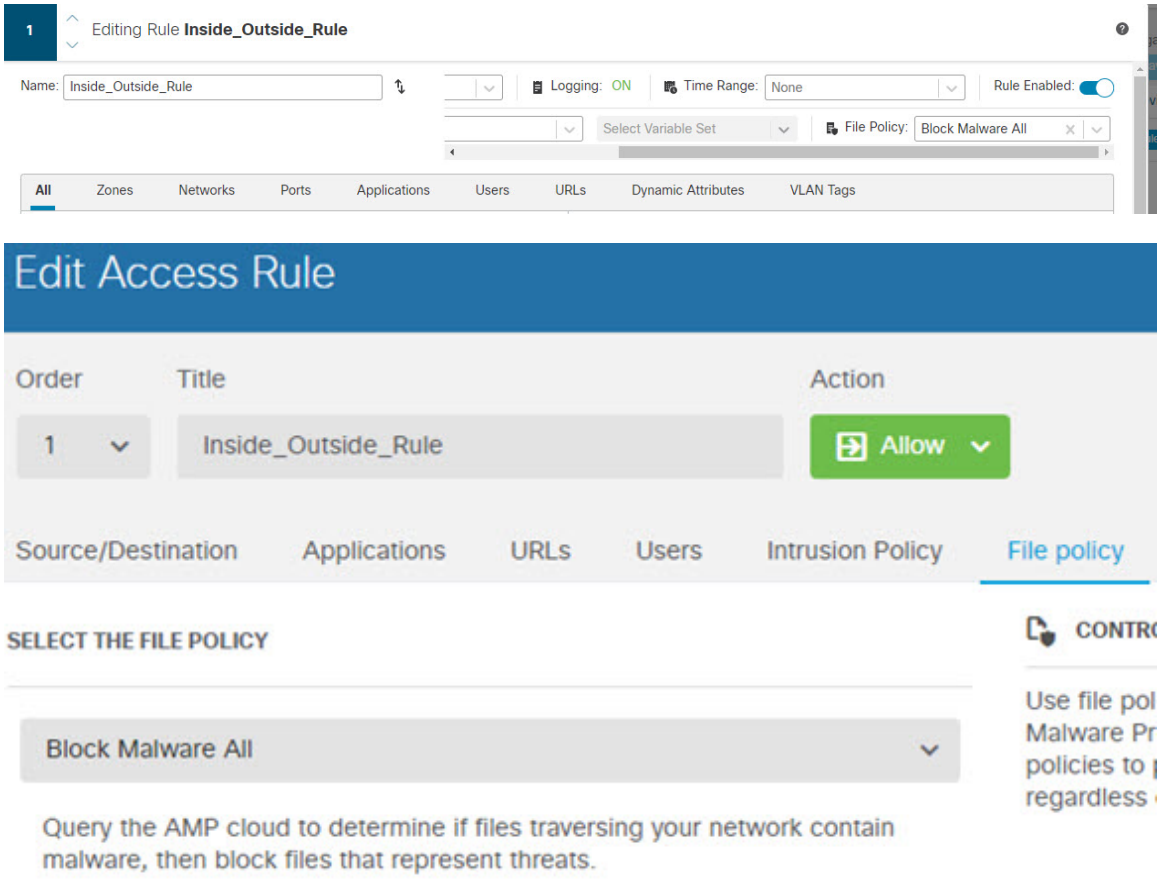
d) Cliquez sur l'onglet **File Policy** (politique de fichiers).

e) Cliquez sur la politique de fichiers que vous souhaitez utiliser.

Vous avez principalement le choix entre **bloquer tous les programmes malveillants**, qui supprime tous les fichiers considérés comme des programmes malveillants, et la fonction **tous les chercher sur le Cloud** , qui interroge le Cisco AMP Cloud pour déterminer la disposition du fichier, mais qui n'en bloque aucun. Si vous souhaitez d'abord voir comment les fichiers sont évalués, utilisez la recherche dans le nuage. Vous pourrez passer à la politique de blocage ultérieurement si vous êtes satisfait de l'évaluation des fichiers.

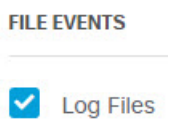
Il existe d'autres politiques qui bloquent les logiciels malveillants. Ces politiques sont associées au contrôle des fichiers, ce qui bloque le téléchargement de documents Microsoft Office, Office ou PDF. Autrement dit, ces politiques empêchent les utilisateurs d'envoyer ces types de fichiers à d'autres réseaux en plus de bloquer les logiciels malveillants. Vous pouvez sélectionner ces politiques si elles répondent à vos besoins.

Pour cet exemple, sélectionnez **Block Malware All**.



f) Cliquez sur l'onglet **Logging** (journalisation) et vérifiez que **Log Files** (fichiers journaux) est sélectionné sous File Events (événements de fichiers).

Par défaut, la journalisation des fichiers est activée lorsque vous sélectionnez une politique de fichiers. Vous devez activer la journalisation des fichiers pour obtenir des informations sur les fichiers et les logiciels malveillants dans les événements et les tableaux de bord.



g) Cliquez sur **OK** pour enregistrer la modification

Étape 3 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Prochaine étape

À ce stade, si des fichiers ou des logiciels malveillants sont transmis, les événements et les tableaux de bord de surveillance devraient commencer à afficher des informations sur les types de fichiers et les événements de fichiers et de logiciels malveillants. Vous pouvez évaluer ces informations pour déterminer si votre réseau a besoin de faire l'objet de plus de précautions de sécurité liées aux transmissions de fichiers.

Comment mettre en œuvre une politique d'utilisation acceptable (filtrage d'URL)

Vous pouvez avoir une politique d'utilisation acceptable pour votre réseau. Les politiques d'utilisation acceptable établissent une distinction entre l'activité réseau appropriée dans votre organisation et l'activité jugée inappropriée. Ces politiques sont généralement axées sur l'utilisation d'Internet et visent à maintenir la productivité, à éviter les responsabilités légales (par exemple, à maintenir un lieu de travail non hostile) et, en général, à contrôler le trafic Web.

Vous pouvez utiliser le filtrage d'URL pour définir une politique d'utilisation acceptable avec des politiques d'accès. Vous pouvez filtrer les grandes catégories, comme les jeux de hasard (Gambling), afin de ne pas avoir à identifier chaque site Web qui doit être bloqué. Pour les correspondances de catégorie, vous pouvez également spécifier la réputation relative des sites à autoriser ou à bloquer. Si un utilisateur tente de rechercher une URL avec cette catégorie et cette combinaison de réputation, la session est bloquée.

L'utilisation des données de catégorie et de réputation simplifie également la création et l'administration des politiques. Cela assure que le système contrôlera le trafic Web comme prévu. Enfin, comme les renseignements sur les menaces de Cisco sont continuellement mis à jour à la lumière de nouvelles URL, ainsi que de nouvelles catégories et risques pour les URL existantes, vous pouvez vous assurer que le système utilise des informations à jour pour filtrer les URL demandées. Les sites malveillants qui représentent des menaces de sécurité, comme

les logiciels malveillants, les pourriels, les réseaux de zombies et l'hameçonnage peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer de nouvelles politiques.

La procédure suivante explique comment mettre en œuvre une politique d'utilisation acceptable en utilisant le filtrage d'URL. Pour les besoins de cet exemple, nous bloquerons les sites de toute réputation dans plusieurs catégories, les sites de réseaux sociaux à risque et un site non classé, badsite.example.com.

Procédure

Étape 1 Si vous ne l'avez pas encore fait, activez la licence **URL**.

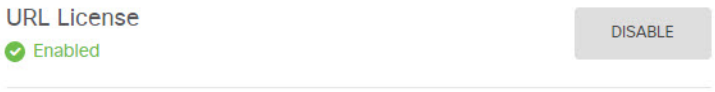
Vous devez activer la licence URL pour utiliser la catégorie URL et les informations de réputation, ou pour voir les informations dans les tableaux de bord et les événements. Si vous utilisez actuellement la licence d'évaluation, vous activez une version d'évaluation de la licence. Si vous avez enregistré l'appareil, vous devez acheter la licence requise et l'ajouter à votre compte Smart Software Manager sur Cisco.com.

a) Cliquez sur **Device (périphérique)**.
b) Cliquez sur **View Configuration** dans le groupe des licences Smart.



c) Cliquez sur **Enable** (activer) dans le groupe **URL** (licence URL).

Le système enregistre la licence avec votre compte ou active la licence d'évaluation, selon le cas. Le groupe doit indiquer que la licence est activée, et le bouton indique Disable (désactivé).



Étape 2 Créez une règle de contrôle d'accès de filtrage d'URL.

Vous voudrez peut-être d'abord voir les catégories des sites visités par vos utilisateurs avant de définir une règle de blocage. Si tel est le cas, vous pouvez créer une règle avec l'action d'autorisation (Allow) pour une catégorie acceptable, comme la catégorie des services financiers (Finance). Étant donné que toutes les connexions Web doivent être inspectées pour déterminer si l'URL appartient à cette catégorie, vous obtiendrez des renseignements sur la catégorie même pour les sites des services non financiers (non-Finance).

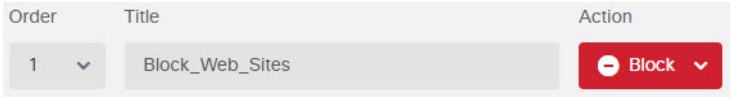
Mais il y a probablement des catégories d'URL dont vous savez déjà que vous souhaitez les bloquer. Une politique de blocage oblige également l'inspection, de sorte que vous obtenez des informations sur les catégories de connexions aux catégories non bloquées, et pas seulement au sujet des catégories bloquées.

a) Cliquez sur **Policies** (politiques) dans le menu principal.

Assurez-vous que la politique de contrôle d'accès (**Access Control**) est affichée.

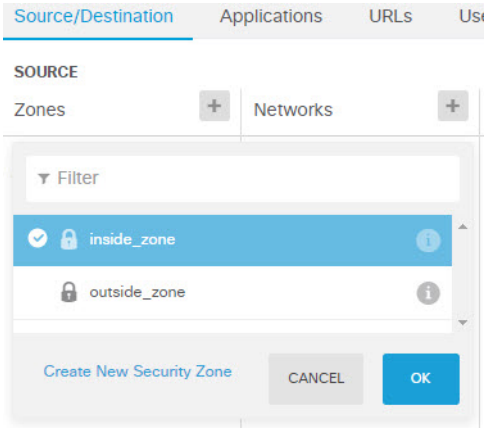
b) Cliquez sur + pour ajouter une nouvelle règle.
c) Configurez l'ordre, le titre et l'action.

- **Order** (ordre) : la valeur par défaut consiste à ajouter de nouvelles règles à la fin de la politique de contrôle d'accès. Cependant, vous devez placer cette règle avant (au-dessus) de toute règle qui correspondrait à la même source ou destination et à d'autres critères, sinon la règle ne sera jamais mise en correspondance (une connexion se conforme à une seule règle, c.-à-d. la première règle à laquelle elle correspond dans le tableau). Pour cette règle, nous utiliserons la même source/destination que la règle Inside_Outside_Rule créée lors de la configuration initiale de l'appareil. Vous avez peut-être également créé d'autres règles également. Pour maximiser l'efficacité du contrôle d'accès, il est préférable d'établir des règles précises dès le début, afin de déterminer rapidement si une connexion est autorisée ou interrompue. Dans cet exemple, sélectionnez **1** comme ordre des règles.
- **Title** (titre) : Donnez un nom significatif à la règle, par exemple Block_Web_Sites.
- **Action** : Sélectionnez **Block**.

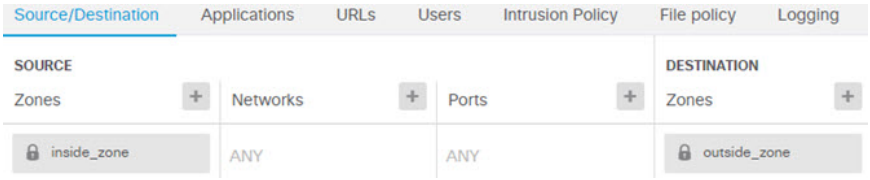


d) Dans l'onglet **Source/Destination**, cliquez sur **+** pour **Source** > **Zones**, sélectionnez **inside_zone**, puis cliquez sur **OK** dans la boîte de dialogue des zones.

L'ajout de l'un des critères fonctionne de la même manière. Cliquez sur **+** pour ouvrir une petite boîte de dialogue où vous cliquez sur les éléments que vous souhaitez ajouter. Vous pouvez cliquer sur plusieurs éléments, puis cliquer sur un élément sélectionné le désélectionne; les cases à cocher indiquent les éléments sélectionnés. Mais rien n'est ajouté à la politique jusqu'à ce que vous cliquiez sur le bouton **OK**; la simple sélection des éléments ne suffit pas.



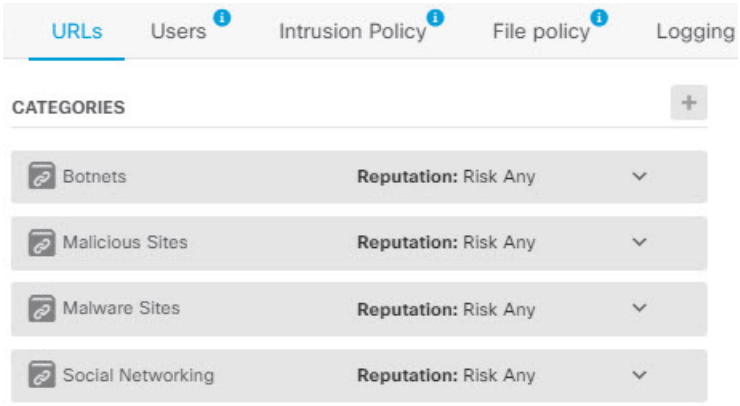
e) En utilisant la même technique, sélectionnez **outside_zone** pour les zones de destination (**Destination** > **Zones**).



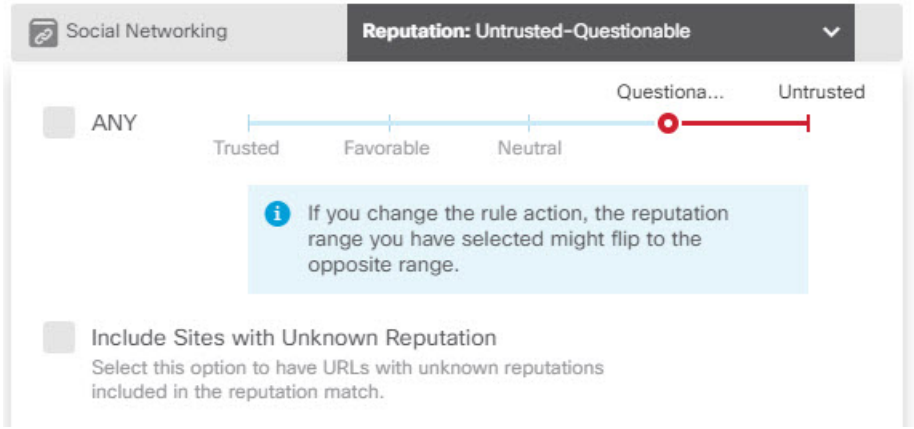
f) Cliquez sur l'onglet **URL**.

g) Cliquez sur le signe + pour les catégories (**Categories**), puis sélectionnez les catégories que vous souhaitez bloquer complètement ou partiellement.

Pour les besoins de cet exemple, sélectionnez réseaux de zombies, sites malveillants, programmes malveillants et réseaux sociaux (Botnets, Malicious Sites, Malware Sites et Social Networking). Il y a d'autres catégories que vous voudrez probablement bloquer. Si vous connaissez un site que vous souhaitez bloquer, mais que vous n'êtes pas sûr de la catégorie, entrez l'URL dans le champ **URL to Check** (URL à vérifier) et cliquez sur **Go** pour lancer la vérification. Vous serez redirigé vers un site Web qui affiche les résultats de la recherche.



h) Pour mettre en œuvre le blocage sensible à la réputation de la catégorie des réseaux sociaux, cliquez sur **Reputation: Risk Any** dans cette catégorie, puis décocher **Any**, avant de sélectionner **Questionable**. Cliquez en dehors de la case du curseur pour le fermer.



À la gauche du curseur de réputation, vous trouverez de l'information sur les sites qui seront autorisés, tandis que les sites qui sont bloqués sont présentés du côté droit. Dans ce cas, seuls les sites de réseaux sociaux ayant une réputation considérée comme douteuse (Questionable) et non fiable (Untrusted) seront bloqués. Ainsi, vos utilisateurs devraient pouvoir accéder aux sites de réseaux sociaux les plus utilisés, où les risques sont moindres.

Sélectionnez l'option **Include Sites with Unknown Reputation** (inclure les sites avec une réputation inconnue) pour inclure les URL de réputation inconnue dans la correspondance de réputation. Les nouveaux sites ne sont généralement pas classés, et il peut y avoir d'autres raisons pour lesquelles la réputation d'un site est inconnue ou ne peut être déterminée.

Grâce à l'information sur la réputation, vous pouvez bloquer sélectivement les sites dans une catégorie que vous souhaitez autoriser autrement.

i) Cliquez sur le **+** à côté de la liste des **URL** à gauche de la liste des catégories.

j) Au bas de la boîte de dialogue contextuelle, cliquez sur le lien **Create New URL** (créer une URL).

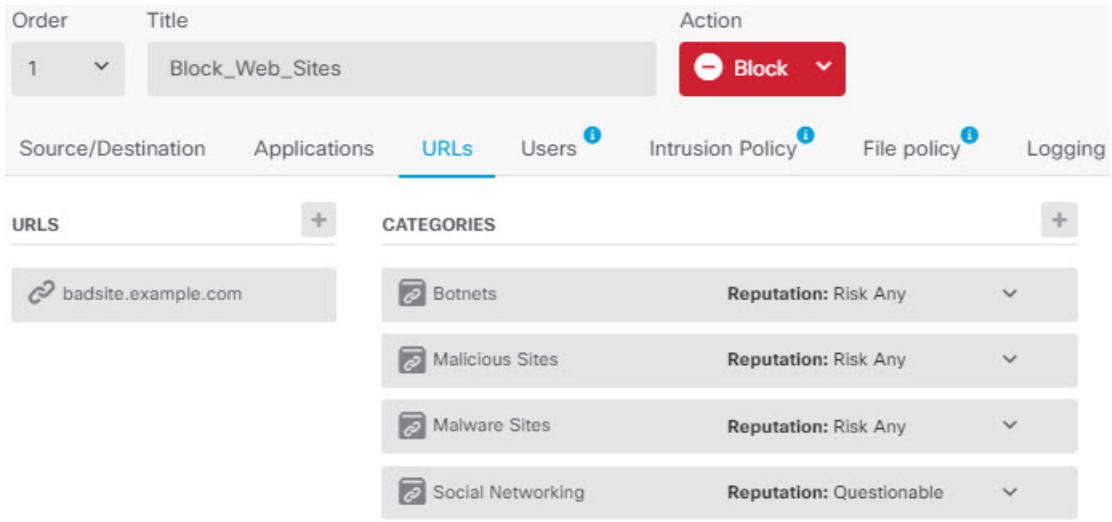
k) Entrez **badsite.exemple.com** pour le nom et l'URL, puis cliquez sur **OK** pour créer l'objet.

Vous pouvez nommer l'objet comme l'URL ou donner un nom différent à l'objet. Pour l'URL, n'incluez pas la partie protocole de l'URL, ajoutez simplement le nom du serveur.



l) Sélectionnez le nouvel objet, puis cliquez sur **OK**.

L'ajout de nouveaux objets lors de la modification des politiques ajoute simplement l'objet à la liste. Le nouvel objet n'est pas automatiquement sélectionné.



m) Cliquez sur l'onglet **Logging** (journalisation) et sélectionnez **Select Log Action (choisir l'action de journalisation)** > **At Beginning and End of Connection (au début et à la fin de la connexion)**.

Vous devez activer la journalisation pour obtenir des informations de catégorie et de réputation dans le tableau de bord de catégorie Web et les événements de connexion.

n) Cliquez sur **OK** pour enregistrer la règle.

Étape 3 (Facultatif) Définissez les préférences de filtrage d'URL.

Lorsque vous activez la licence URL, le système active automatiquement les mises à jour de la base de données de catégories Web. Le système recherche les mises à jour toutes les 30 minutes, bien que les données soient généralement mises à jour une fois par jour. Vous pouvez désactiver ces mises à jour si, pour une raison quelconque, vous ne souhaitez pas les mettre en œuvre.

Vous pouvez également choisir d'envoyer à Cisco des URL qui ne sont pas catégorisées pour analyse. Ainsi, si la base de données URL installée ne dispose pas d'une catégorisation pour un établissement, le Cisco Cloud peut en avoir une. Le nuage renvoie la catégorie et la réputation, et vos règles basées sur la catégorie peuvent alors être appliquées correctement à la requête URL. La sélection de cette option est importante pour les systèmes bas de gamme, qui installent une base de données d'URL plus petite en raison de contraintes de mémoire. Vous pouvez définir une durée de vie pour les résultats de la recherche : la valeur par défaut est Never (jamais), ce qui signifie que les résultats de la recherche ne sont jamais actualisés.

a) Cliquez sur **Device (périphérique)**.
b) Cliquez sur **System Settings** > **Traffic Settings** > **URL Filtering Preferences**.
c) Sélectionnez **Query Cisco CSI for Unknown URLs** (interroger Cisco CSI pour les URL inconnues).
d) Sélectionnez une durée de vie URL raisonnable (**URL Time to Live**), par exemple 24 heures.
e) Cliquez sur **Save** (Enregistrer).

Étape 4 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Prochaine étape

À ce stade, les tableaux de bord et les événements de surveillance devraient commencer à afficher des informations sur les réputations et les catégories web et sur les connexions abandonnées. Vous pouvez évaluer ces informations pour déterminer si votre filtrage d'URL abandonne uniquement les sites qui sont répréhensibles, ou si vous avez besoin d'assouplir les paramètres de réputation pour certaines catégories.

Pensez à informer les utilisateurs au préalable que vous allez bloquer l'accès aux sites Web en fonction de leur catégorie et de leur réputation.

Comment contrôler l'utilisation des applications

Le Web est une plateforme désormais omniprésente pour la distribution des applications dans l'entreprise, qu'il s'agisse de plateformes d'applications basées sur un navigateur Web ou d'applications multimédias qui utilisent des protocoles Web pour l'entrée et la sortie des réseaux d'entreprise.

FTD inspecte les connexions pour déterminer l'application utilisée. Cela permet d'établir des règles de contrôle d'accès ciblées sur les applications, plutôt que de cibler des ports TCP/UDP spécifiques. Ainsi, vous pouvez bloquer ou autoriser sélectivement les applications Web même si elles utilisent le même port.

Bien que vous puissiez sélectionner des applications spécifiques à autoriser ou à bloquer, vous pouvez également rédiger des règles en fonction du type, de la catégorie, de l'étiquette, du risque ou de la pertinence de l'entreprise. Par exemple, vous pouvez créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible pertinence commerciale. Si un utilisateur tente d'utiliser l'une de ces applications, la session est bloquée.

Cisco procède fréquemment à la mise à jour ou à l'ajout de détecteurs d'applications supplémentaires au moyen des mises à jour du système et de la base de données sur les vulnérabilités (VDB). Ainsi, une règle bloquant les applications à risque élevé peut s'appliquer automatiquement aux nouvelles applications sans que vous ayez à mettre à jour la règle manuellement.

Dans ce scénario, nous bloquerons toute application appartenant à la catégorie **anonymizer/proxy** (anonymiseur/serveur mandataire).

Avant de commencer

Ce scénario se fonde sur l'hypothèse voulant que vous ayez terminé le scénario Comment mieux comprendre le trafic de votre réseau, à la page 49. Le scénario explique comment recueillir des informations sur l'utilisation des applications, que vous pouvez analyser dans le tableau de bord des applications. La compréhension des applications réellement utilisées peut vous aider à concevoir des règles efficaces basées sur les applications. Le scénario explique également comment planifier les mises à jour de la VDB, qui ne seront pas reproduites ici. Assurez-vous de mettre à jour la VDB régulièrement afin que les applications puissent être correctement identifiées.

Procédure

Étape 1 Créez la règle de contrôle d'accès basée sur l'application.

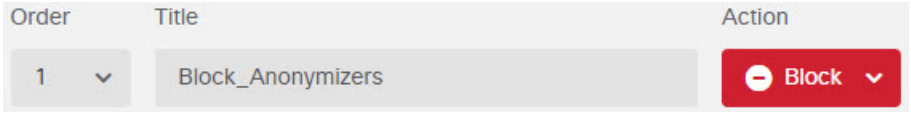
a) Cliquez sur **Policies** (politiques) dans le menu principal.

Assurez-vous que la politique de contrôle d'accès (**Access Control**) est affichée.

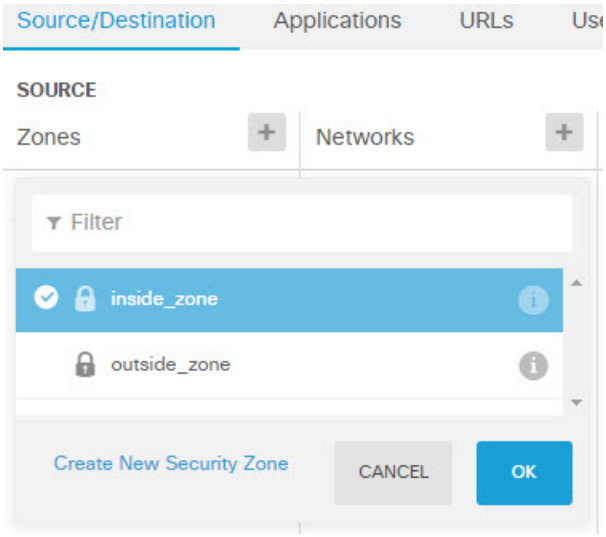
b) Cliquez sur + pour ajouter une nouvelle règle.

c) Configurez l'ordre, le titre et l'action.

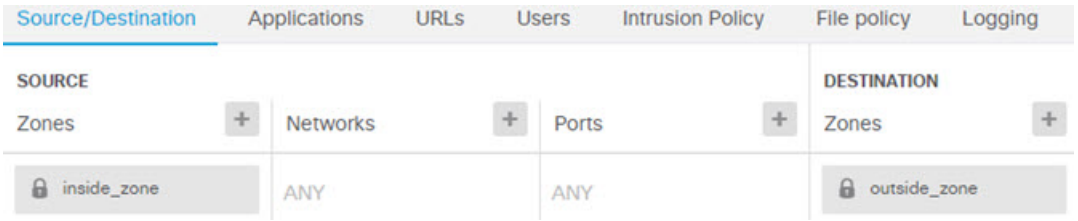
- **Order** (ordre) : la valeur par défaut consiste à ajouter de nouvelles règles à la fin de la politique de contrôle d'accès. Cependant, vous devez placer cette règle avant (au-dessus) de toute règle qui correspondrait à la même source ou destination et à d'autres critères, sinon la règle ne sera jamais mise en correspondance (une connexion se conforme à une seule règle, c.-à-d. la première règle à laquelle elle correspond dans le tableau). Pour cette règle, nous utiliserons la même source/destination que la règle Inside_Outside_Rule créée lors de la configuration initiale de l'appareil. Vous avez peut-être également créé d'autres règles également. Pour maximiser l'efficacité du contrôle d'accès, il est préférable d'établir des règles précises dès le début, afin de déterminer rapidement si une connexion est autorisée ou interrompue. Dans cet exemple, sélectionnez **1** comme ordre des règles.
- **Title** (titre) : Donnez un nom significatif à la règle, par exemple Block_Anonymizers.
- **Action** : Sélectionnez **Block**.



d) Dans l'onglet **Source/Destination**, cliquez sur **+** pour **Source** > **Zones**, sélectionnez **inside_zone**, puis cliquez sur **OK** dans la boîte de dialogue des zones.



e) En utilisant la même technique, sélectionnez **outside_zone** pour les zones de destination (**Destination** > **Zones**).



f) Cliquez sur l'onglet **Applications**.

g) Cliquez sur le signe **+** pour les **Applications**, puis cliquez sur le lien **Advanced Filter** (filtre avancé) au bas de la boîte de dialogue contextuelle.

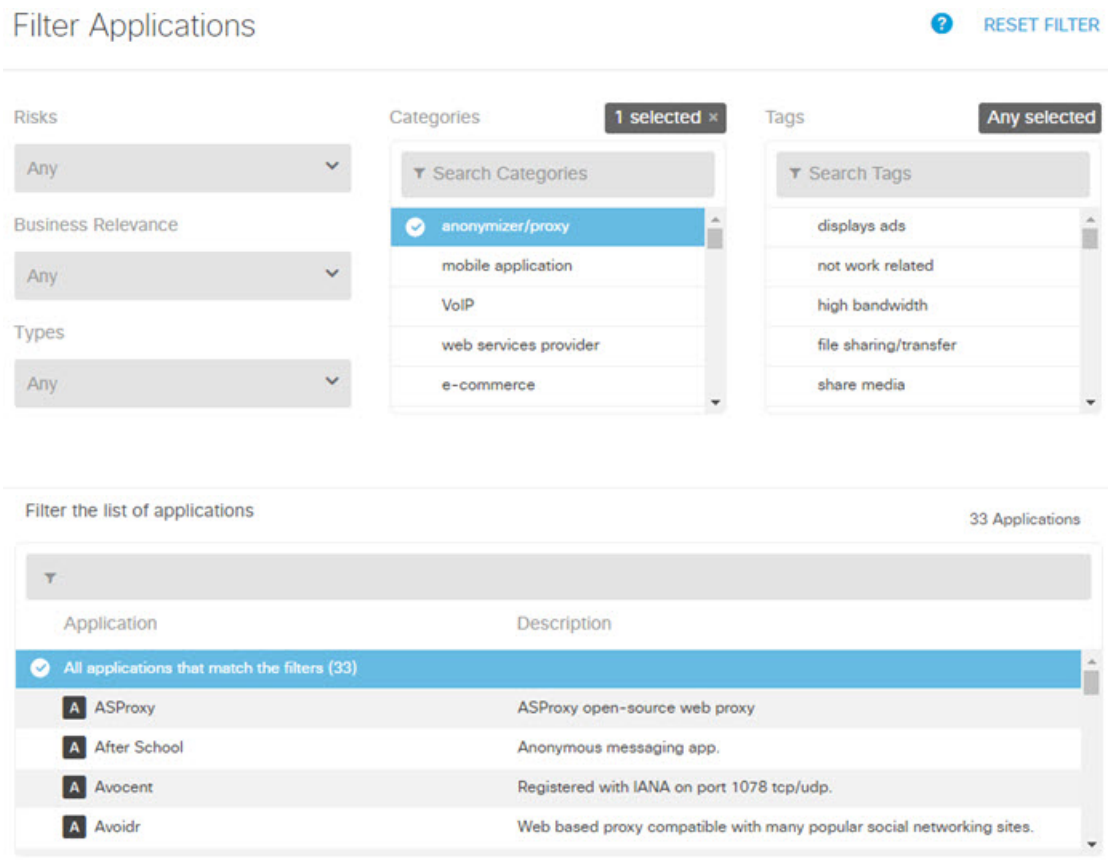
Bien que vous puissiez créer des objets de filtre d'application au préalable et les sélectionner dans la liste des filtres d'application ici, vous pouvez également spécifier des critères directement dans la règle de contrôle d'accès, et éventuellement enregistrer les critères en tant qu'objet de filtre. À moins d'écrire une règle pour une seule application, il est plus facile d'utiliser la boîte de dialogue de filtre avancé (Advanced Filter) pour trouver des applications et créer des critères appropriés.

À mesure que vous sélectionnez des critères, la liste des applications au bas de la boîte de dialogue est mise à jour pour afficher avec exactitude les applications qui correspondent aux critères. La règle que vous établissez s'applique à ces applications.

Examinez attentivement cette liste. Par exemple, vous pourriez être tenté de bloquer toutes les applications à très haut risque. Cependant, à ce jour, l'application TFPT est considérée comme à très haut risque. La plupart des entreprises ne veulent pas bloquer cette application. Prenez le temps

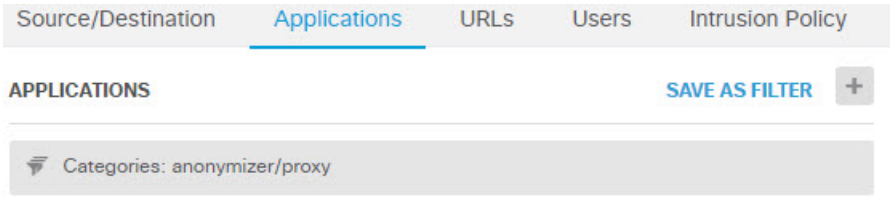
d'expérimenter en adoptant différents critères de filtrage pour voir quelles applications correspondent à vos sélections. Gardez à l'esprit que ces listes peuvent changer à chaque mise à jour de VDB.

Pour les besoins de cet exemple, sélectionnez les anonymiseurs et serveurs mandataires (anonymizers/proxies) dans la liste des catégories (Categories).



h) Cliquez sur **Add** (ajouter) dans la boîte de dialogue des filtres avancés (Advanced Filters).

Le filtre est ajouté et affiché sous l'onglet Applications.



i) Cliquez sur l'onglet **Logging** (journalisation) et sélectionnez **Select Log Action (choisir l'action de journalisation)** > **At Beginning and End of Connection (au début et à la fin de la connexion)**.

Vous devez activer la journalisation pour obtenir des informations sur les connexions bloquées par cette règle.

j) Cliquez sur **OK** pour enregistrer la règle.

Étape 2 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Étape 3 Cliquez sur **Monitoring** (suivi) et évaluez les résultats.

Vous pouvez maintenant voir les connexions abandonnées sur le widget Applications du tableau de bord **Network Overview** (aperçu du réseau). Utilisez les options déroulantes **All/Denied/Allowed** pour vous concentrer uniquement sur les applications abandonnées.

Vous pouvez également trouver des informations sur les applications sur le tableau de bord des applications Web (**Web Applications**). Les tableaux de bord **Applications** affichent les résultats liés au protocole. Si une personne tente d'utiliser ces applications, en supposant que vous avez activé les politiques d'identité et exigez une authentification, vous devriez être en mesure d'établir un lien entre l'application et l'utilisateur qui tente la connexion.

Comment ajouter un sous-réseau

Si une interface est disponible sur votre appareil, vous pouvez la connecter à un commutateur (ou à un autre routeur) pour fournir des services à un autre sous-réseau.

Il y a plusieurs raisons pour lesquelles vous pourriez souhaiter ajouter un sous-réseau. Pour ce scénario d'utilisation, nous aborderons le scénario typique suivant.

- Le sous-réseau est un réseau interne qui utilise le réseau privé 192.168.2.0/24.
- L'interface du réseau a l'adresse statique 192.168.2.1. Dans cet exemple, l'interface physique est dédiée au réseau. Une autre option consiste à utiliser une interface déjà câblée et à créer une sous-interface pour le nouveau réseau.
- Le périphérique fournira des adresses aux postes de travail sur le réseau au moyen de DHCP, en utilisant 192.168.2.2-192.168.2.254 comme ensemble d'adresses.
- L'accès réseau aux autres réseaux internes et au réseau externe sera autorisé. Le trafic vers le réseau externe utilisera NAT pour obtenir une adresse publique.



Remarque Cet exemple suppose que l'interface inutilisée ne fait pas partie d'un groupe de ponts. S'il s'agit actuellement d'un membre du groupe de ponts, vous devez d'abord le retirer du groupe de ponts avant de suivre cette procédure.

Avant de commencer

Connectez physiquement le câble réseau à l'interface et au commutateur du nouveau sous-réseau.

Procédure

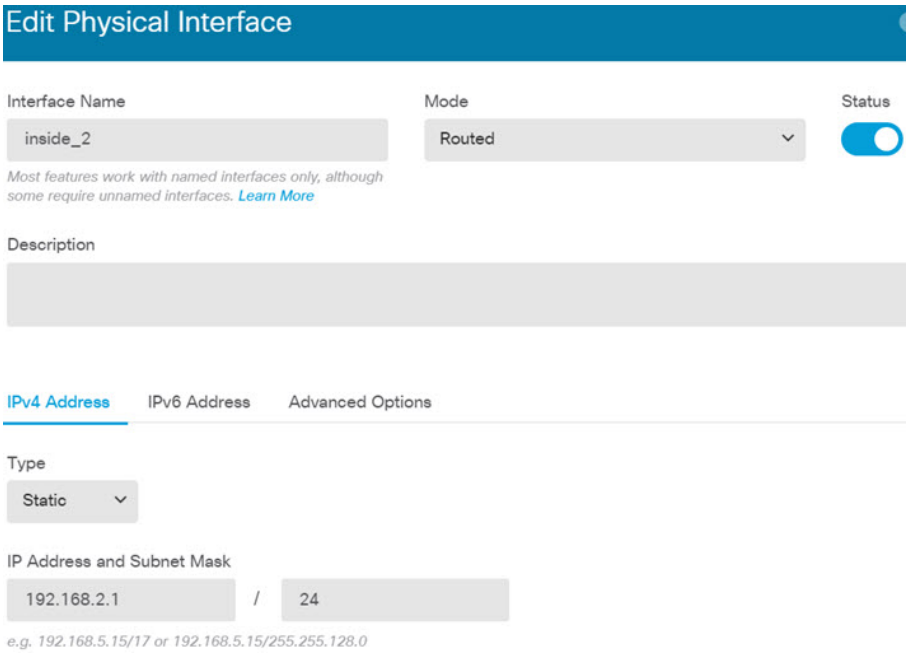
Étape 1 Configurez l'interface.

a) Cliquez sur **Device** (périphérique), cliquez sur le lien dans le résumé des **Interfaces**. Cliquez ensuite sur le type d'interfaces pour consulter la liste des interfaces.

b) Passez la souris sur la cellule **Actions** sur le côté droit de la ligne pour l'interface que vous avez câblée, puis cliquez sur l'icône de modification ( ).

c) Configurez les propriétés de base de l'interface.

- **Name** (nom) : Un nom unique pour l'interface. Dans cet exemple, le nom sera **inside_2**.
- **Mode** : Sélectionnez **Routed** (routage).
- **Status** (état) : Cliquez sur le bouton d'état pour activer l'interface.
- Onglet **IPv4 Address** : Sélectionnez **Static** (statique) pour le **Type**, puis entrez **192.168.2.1/24**.



d) Cliquez sur **Save** (Enregistrer).

La liste des interfaces affiche l'état de l'interface mis à jour et l'adresse IP configurée.



Étape 2 Configurez le serveur DHCP pour l'interface.

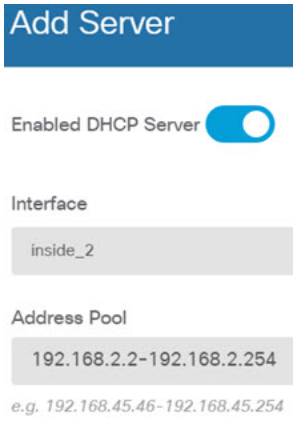
a) Cliquez sur **Device (périphérique)**.

b) Cliquez sur **System Settings (paramètres système)** > **DHCP Server (serveur DHCP)**.
c) Cliquez sur l'onglet **DHCP Servers** (serveurs DHCP).

Le tableau répertorie tous les serveurs DHCP existants. Si vous utilisez la configuration par défaut, la liste en comprend une pour l'interface interne.

d) Cliquez sur + au-dessus du tableau.
e) Configurez les propriétés du serveur.

- **Enable DHCP Server (activer le serveur DHCP)** : Ce bouton permet d'activer le serveur.
- **Interface** : Sélectionnez l'interface sur laquelle vous fournissez des services DHCP. Dans cet exemple, sélectionnez inside_2.
- **Address Pool** (ensemble d'adresse) : Les adresses que le serveur peut fournir aux périphériques du réseau. Entrez 192.168.2.2-192.168.2.254. Assurez-vous de ne pas inclure l'adresse réseau (.0), l'adresse d'interface (.1) ou l'adresse de diffusion (.255). En outre, si vous avez besoin d'adresses statiques pour des périphériques sur le réseau, excluez ces adresses du groupe. Le pool doit être composé d'une seule série continue d'adresses. Choisissez donc des adresses statiques en début ou en fin de plage.



f) Cliquez sur **Add** (ajouter).



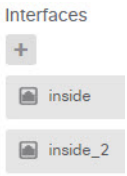
#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL
1	inside	Enabled	192.168.1.5-192.168.1.254
2	inside_2	Enabled	192.168.2.2-192.168.2.254

Étape 3 Ajoutez l'interface à la zone de sécurité interne.

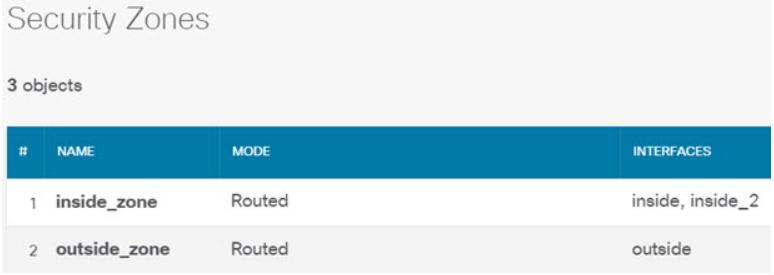
Pour établir des politiques sur une interface, l'interface doit appartenir à une zone de sécurité. Vous établissez des politiques pour les zones de sécurité. Ainsi, lorsque vous ajoutez et supprimez des interfaces dans les zones, vous modifiez automatiquement les politiques appliquées à l'interface.

a) Cliquez sur **Objects** (objets) dans le menu principal.
b) Sélectionnez **Security Zones** (zones de sécurité) dans la table des matières.
c) Passez la souris sur la cellule **Actions** sur le côté droit de la ligne pour l'objet **inside_zone**, puis cliquez sur l'icône de modification ( ).

d) Cliquez sur + sous **Interfaces**, sélectionnez l'interface inside_2, puis cliquez sur **OK** dans la liste des interfaces.



e) Cliquez sur **Save** (Enregistrer).



Étape 4 Créez une règle de contrôle d'accès qui autorise le trafic entre les réseaux internes.

Le trafic n'est pas autorisé automatiquement entre les interfaces. Vous devez créer des règles de contrôle d'accès pour autoriser le trafic que vous souhaitez. La seule exception : si vous autorisez le trafic dans l'action par défaut de la règle de contrôle d'accès. Pour les besoins de cet exemple, nous supposerons que vous avez conservé l'action de blocage par défaut que l'assistant de configuration de périphérique configure. Ainsi, vous devez créer une règle qui autorisera le trafic entre les interfaces internes. Si vous avez déjà créé une règle comme celle-ci, ignorez cette étape.

a) Cliquez sur **Policies** (politiques) dans le menu principal.

Assurez-vous que la politique de contrôle d'accès (**Access Control**) est affichée.

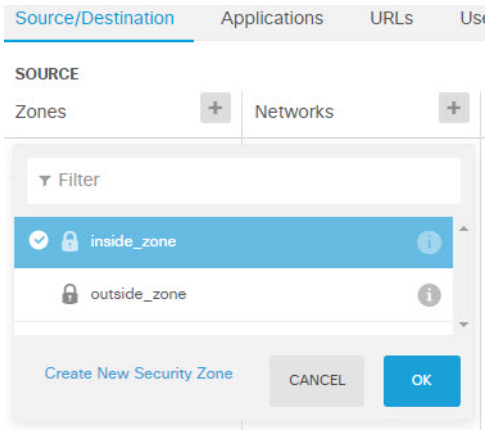
b) Cliquez sur + pour ajouter une nouvelle règle.

c) Configurez l'ordre, le titre et l'action.

- **Order** (ordre) : la valeur par défaut consiste à ajouter de nouvelles règles à la fin de la politique de contrôle d'accès. Cependant, vous devez placer cette règle avant (au-dessus) de toute règle qui correspondrait à la même source ou destination et à d'autres critères, sinon la règle ne sera jamais mise en correspondance (une connexion se conforme à une seule règle, c.-à-d. la première règle à laquelle elle correspond dans le tableau). Pour cette règle, nous utiliserons des critères de Source/Destination uniques, donc l'ajout de la règle à la fin de la liste est acceptable.
- **Title** (title) : Attribuez un nom significatif à la règle, par exemple Allow_Inside_Inside.
- **Action** : Sélectionnez **Allow** (autoriser).

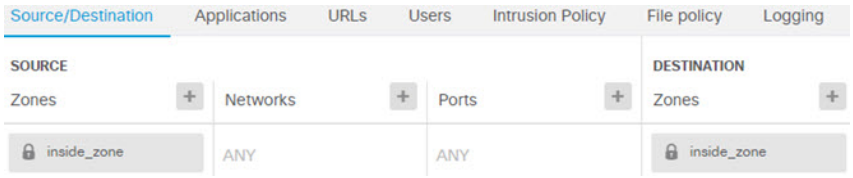


d) Dans l'onglet **Source/Destination**, cliquez sur + pour **Source** > **Zones**, sélectionnez **inside_zone**, puis cliquez sur **OK** dans la boîte de dialogue des zones.



e) Selon cette même méthode, pour définir les zones de destination, sélectionnez **inside_zone** sous **Destination** > **Zones**.

Une zone de sécurité doit contenir au moins deux interfaces pour sélectionner la même zone pour la source et la destination.



f) (Facultatif) Configurez l'inspection des intrusions et des logiciels malveillants.

Bien que les interfaces internes se trouvent dans une zone de confiance, il est courant que les utilisateurs connectent des ordinateurs portables au réseau. Ainsi, un utilisateur pourrait inconsciemment introduire une menace à l'intérieur de votre réseau à partir d'un réseau externe ou d'un point d'accès Wi-Fi. Vous pouvez rechercher les intrusions et les logiciels malveillants dans le trafic entre vos réseaux internes.

Pensez à faire ce qui suit.

- Cliquez sur l'onglet **Intrusion Policy** (politique de prévention des intrusions) et activez la politique, et sélectionnez la politique Balanced Security and Connectivity (équilibre entre la sécurité et la connectivité).
- Cliquez sur l'onglet **File Policy**, puis sélectionnez la politique visant à bloquer les logiciels malveillants (Block Malware All).

g) Cliquez sur l'onglet **Logging** (journalisation) et sélectionnez **Select Log Action (choisir l'action de journalisation)** > **At Beginning and End of Connection (au début et à la fin de la connexion)**.

Vous devez activer la journalisation pour obtenir des informations sur les connexions qui correspondent à cette règle. La journalisation ajoute des statistiques au tableau de bord et affiche les événements dans le visualiseur d'événements.

h) Cliquez sur **OK** pour enregistrer la règle.

Étape 5 Vérifiez que les politiques requises sont définies pour le nouveau sous-réseau.

En ajoutant l'interface à la zone de sécurité inside_zone, toutes les politiques existantes pour inside_zone s'appliquent automatiquement au nouveau sous-réseau. Cependant, prenez le temps d'inspecter vos politiques et assurez-vous qu'aucune politique supplémentaire n'est nécessaire.

Si vous avez terminé la configuration initiale de l'appareil, les politiques suivantes devraient déjà s'appliquer.

- **Access Control** (contrôle d'accès) : La règle Inside_Outside_Règlement devrait autoriser tout le trafic entre le nouveau sous-réseau et le réseau externe. Si vous avez suivi les scénarios d'utilisation précédents, la politique prévoit également une inspection des intrusions et des logiciels malveillants. Vous devez établir une règle qui autorise le trafic entre le nouveau réseau et le réseau externe, sinon les utilisateurs ne peuvent pas accéder à Internet ou à d'autres réseaux externes.
- **NAT** : La règle InsideOutsideNATrule s'applique à n'importe quelle interface allant vers l'interface externe et applique la PAT d'interface. Si vous respectez cette règle, le trafic du nouveau réseau vers l'extérieur verra l'adresse IP traduite en un port unique sur l'adresse IP de l'interface externe. Si vous n'avez pas de règle qui s'applique à toutes les interfaces ou aux interfaces inside_zone, lorsque vous passez à l'interface externe, vous devrez peut-être en créer une maintenant.
- **Identity** (identity) : Aucune politique d'identité par défaut n'a été établie. Cependant, si vous avez suivi les scénarios d'utilisation précédents, vous pourriez avoir une politique d'identité qui nécessite déjà une authentification pour le nouveau réseau. Si aucune politique d'identité ne s'applique, créez-en une maintenant si vous souhaitez obtenir des informations basées sur l'utilisateur pour le nouveau réseau.

Étape 6 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Prochaine étape

Vérifiez que les stations de travail du nouveau sous-réseau obtiennent des adresses IP à l'aide de DHCP et qu'elles peuvent atteindre d'autres réseaux internes et externes. Utilisez les tableaux de bord de surveillance et le visualiseur d'événements pour évaluer l'utilisation du réseau.

Comment surveiller passivement le trafic sur un réseau

Un périphérique Firepower Threat Defense est normalement déployé comme pare-feu actif et dispositif de sécurité IPS (système de prévention des intrusions). La fonction principale de l'appareil est de fournir une protection active au réseau en supprimant les connexions indésirables et les menaces.

Cependant, vous pouvez également déployer le système en mode passif. Dans ce mode, l'appareil analyse simplement le trafic sur les ports de commutation surveillés. Ce mode se destine principalement à des fins de démonstration ou de test. Il vous permet de vous familiariser avec le périphérique avant de le déployer en tant

que pare-feu actif. Grâce à un déploiement passif, vous pouvez surveiller les types de menaces qui apparaissent sur le réseau, les catégories d'URL parcourues par les utilisateurs, etc.

Bien que vous utilisiez normalement le mode passif à des fins de démonstration ou de test uniquement, vous pouvez également utiliser le mode passif dans un environnement de production s'il fournit un service dont vous avez besoin, tel que l'IDS (système de détection des intrusions sans prévention). Vous pouvez combiner des interfaces passives avec des interfaces actives de routage de pare-feu pour fournir la combinaison exacte des services requis par votre organisation.

La procédure suivante explique comment déployer le système de manière passive pour analyser le trafic passant par un nombre limité de ports de commutation.

Remarque Cet exemple concerne un périphérique Firepower Threat Defense matériel. Vous pouvez également utiliser le mode passif pour for FTDv, mais la configuration du réseau est différente. Pour de plus amples renseignements, consultez la section Configurer le VLAN pour une interface passive FTDv, à la page 296. Sinon, cette procédure s'applique également à FTDv.

Avant de commencer

Cette procédure suppose que vous avez connecté les interfaces interne et externe et terminé la configuration initiale du périphérique avec l'assistant. Même dans un déploiement passif, vous avez besoin d'une connexion Internet pour télécharger les mises à jour des bases de données du système. Vous devez également être en mesure de vous connecter à l'interface de gestion pour ouvrir Gestionnaire de périphériques de pare-feu, ce que vous pouvez faire au moyen de connexions directes au port intérieur ou de gestion.

Cet exemple suppose également que vous avez activé syslog pour les politiques de prévention des intrusions dans la page **Policies** > **Intrusion**.

Procédure

Étape 1 Configurez un port de commutation comme port SPAN (Switched Port Analyzer) et configurez une session de surveillance pour les interfaces source.

Dans l'exemple suivant, un port SPAN et une session de surveillance sont configurés pour deux interfaces sources sur un commutateur de la gamme Cisco Nexus 5000. Si vous utilisez un type de commutateur différent, les commandes requises pourraient différer.

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

Pour vérifier :

```
switch# show monitor session 1 brief
   session 1
```

```
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

Étape 2 Connectez l'interface Firepower Threat Defense au port SPAN du commutateur.

Il est préférable de sélectionner un port actuellement inutilisé sur le périphérique Firepower Threat Defense. Selon l'exemple de configuration du commutateur, vous devez connecter le câble à l'Ethernet 1/48 du commutateur. Il s'agit de l'interface de destination pour la session de surveillance.

Étape 3 Configurez l'interface Firepower Threat Defense en mode passif.

a) Cliquez sur **Device** (périphérique), puis sur le lien dans le **résumé des** interfaces. Cliquez ensuite sur **Interfaces** ou **EtherChannels**.

b) Cliquez sur l'icône de modification ( ) pour l'interface physique ou le port EtherChannel que vous souhaitez modifier.

Choisissez une interface actuellement inutilisée. Si vous avez l'intention de convertir une interface en cours d'utilisation en interface passive, vous devez d'abord supprimer l'interface de toute zone de sécurité et supprimer toutes les autres configurations qui utilisent l'interface.

c) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

d) Configurez les éléments suivants :

- **Interface Name** : le nom de l'interface (jusqu'à 48 caractères). Les caractères alphabétiques doivent être en minuscules. Par exemple, **surveiller**.
- **Mode** : Sélectionnez **Passive** (passif).



e) Cliquez sur **OK**.

Étape 4 Créez une zone de sécurité passive pour l'interface.

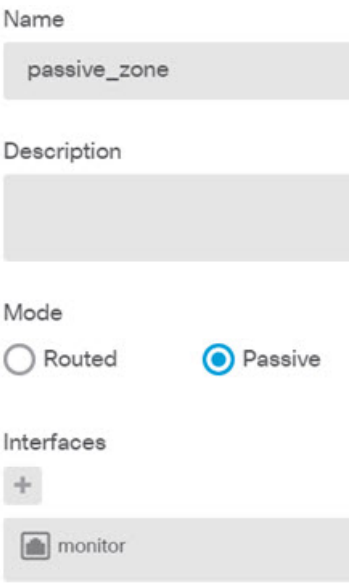
a) Sélectionnez **Objects** (objets), puis **Security Zones** (zones de sécurité) dans la table des matières.

b) Cliquez sur le bouton +.

c) Entrez un nom pour l'objet (sous **Name**) et, facultativement, une description. Par exemple, **passive_zone**.

d) Sous **Mode**, sélectionnez **Passive** (passif).

e) Cliquez sur + et sélectionnez l'interface passive.



f) Cliquez sur **OK**.

Étape 5 Configurez une ou plusieurs règles de contrôle d'accès pour la zone de sécurité passive.

Le nombre et le type de règles que vous créez dépendent des informations que vous souhaitez réunir. Par exemple, si vous souhaitez configurer le système en tant qu'IDS (système de détection des intrusions), vous devez configurer au moins une règle d'autorisation comprenant une politique de prévention des intrusions attribuée. Si vous souhaitez réunir des données sur des catégories d'URL, vous avez besoin d'au moins une règle comprenant une catégorie d'URL précisée.

Vous pouvez créer des règles de blocage pour consulter de l'information sur les connexions que le système aurait bloquées sur une interface à routage actif. Ces connexions ne sont pas bloquées, car l'interface est passive, mais vous verrez clairement comment le système aurait préparé le trafic sur le réseau.

Les scénarios d'utilisation suivants couvrent les principales utilisations des règles de contrôle d'accès. Ceux-ci s'appliquent également aux interfaces passives. Il suffit de sélectionner la zone de sécurité passive comme zone source pour les règles que vous créez.

- Comment bloquer les menaces, à la page 56
- Comment bloquer les logiciels malveillants, à la page 61
- Comment mettre en œuvre une politique d'utilisation acceptable (filtrage d'URL), à la page 64
- Comment contrôler l'utilisation des applications, à la page 69

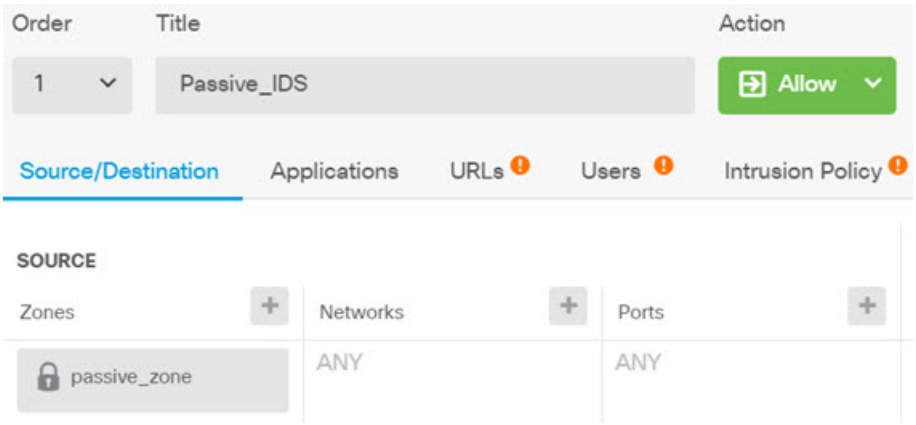
La procédure suivante crée deux règles d'autorisation pour appliquer une politique de prévention des intrusions et pour réunir des données de catégorie d'URL.

a) Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.
b) Cliquez sur le signe plus (+) pour ajouter une règle autorisant tout trafic, mais appliquant une politique de prévention des intrusions.
c) Sélectionnez **1** comme ordre des règles. Cette règle est plus spécifique que la règle par défaut, mais ne la chevauche pas. Si vous avez déjà établi des règles personnalisées, sélectionnez la position appropriée pour que le trafic vers l'interface passive ne corresponde pas à ces règles.
d) Saisissez un nom pour la règle, par exemple **Passive_IDS**.

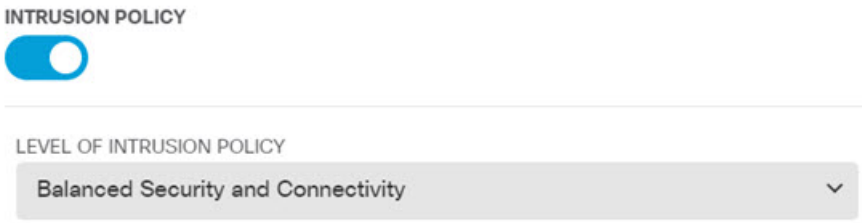
e) Sélectionnez **Allow** (autoriser) sous **Action**.

f) Sous l'onglet **Source/Destination**, sélectionnez la zone passive pour **Source** > **Zones**. Ne configurez aucune autre option pour l'onglet.

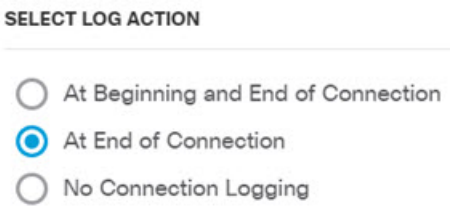
Lors de l'exécution en mode d'évaluation, la règle devrait être la suivante :



g) Cliquez sur l'onglet **Intrusion Policy** (politique de prévention des intrusions), réglez le curseur sur **On** (activée) et sélectionnez une politique de prévention des intrusions, comme la politique **Balanced Security and Connectivity** (équilibre entre la sécurité et la connectivité), qui est recommandée pour la plupart des réseaux.



h) Cliquez sur l'onglet **Logging** (journalisation) et sélectionnez **At End of Connection**(à la fin de la connexion) pour l'option de journalisation.



i) Cliquez sur **OK**.

j) Cliquez sur **+** pour ajouter une règle qui exigera que le système effectue une inspection approfondie pour déterminer l'URL et la catégorie de toutes les requêtes HTTP.

Cette règle vous permet de voir les informations de catégorie d'URL dans les tableaux de bord. Pour économiser du temps de traitement et améliorer les performances, le système détermine la catégorie d'URL uniquement s'il existe au moins une règle de contrôle d'accès qui spécifie une condition de catégorie d'URL.

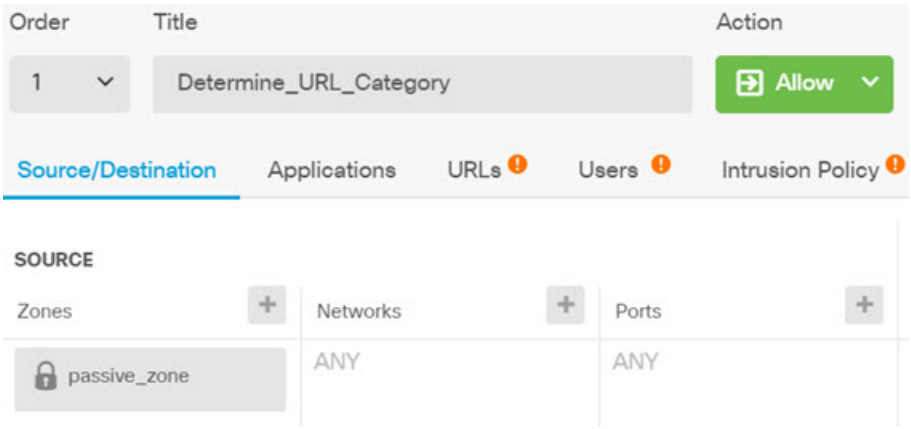
k) Sélectionnez **1** comme ordre des règles. Cela la placera au-dessus de la règle précédente (Passive_IDS). Si vous la placez après cette règle (qui s'applique à tout le trafic), la règle que vous créez maintenant ne sera jamais mise en correspondance.

l) Saisissez un nom pour la règle, par exemple, **Determine_URL_Category**.

m) Sélectionnez **Allow** (autoriser) sous **Action**.

Sinon, vous pouvez sélectionner **Block** (bloquer). L'une ou l'autre des actions permettra d'atteindre votre objectif pour cette règle.

n) Sous l'onglet **Source/Destination**, sélectionnez la zone passive pour **Source** > **Zones**. Ne configurez aucune autre option pour l'onglet.



o) Cliquez sur l'onglet **URL**, cliquez sur le signe plus (+) à côté de **Categories** (catégories), puis sélectionnez l'une des catégories. Par exemple, **Search Engines and Portals (portails et moteurs de recherche)**. Vous pouvez éventuellement sélectionner un niveau de réputation ou le laisser à la valeur par défaut « Any » (n'importe lequel).



p) Cliquez sur l'onglet **Intrusion Policy** (politique de prévention des intrusions), réglez le curseur sur **On** (activée), puis sélectionnez la même politique de prévention que pour la première règle.

q) Cliquez sur l'onglet **Logging** (journalisation) et sélectionnez **At End of Connection**(à la fin de la connexion) pour l'option de journalisation.

Toutefois, si vous avez sélectionné l'action **Block** (bloquer), sélectionnez l'option au début et à la fin de la connexion (**At Beginning and End of Connection**). Comme les connexions bloquées ne sont pas terminées en tant que telles, vous obtenez uniquement des informations de journalisation au début de la connexion.

r) Cliquez sur **OK**.

Étape 6 (Facultatif) Configurer d'autres politiques de sécurité.

Vous pouvez également configurer les politiques de sécurité suivantes pour voir leur incidence sur le trafic :

- **Identity** (identité) : Permet de réunir des renseignements sur l'utilisateur. Vous pouvez configurer dans la politique sur l'identité une règle pour vous assurer que l'identité de l'utilisateur associé à une adresse IP est établie. Le processus de mise en œuvre des politiques sur l'identité pour les interfaces passives est

le même que pour les interfaces de routage. Veuillez suivre le scénario d'utilisation décrit dans Comment mieux comprendre le trafic de votre réseau, à la page 49.

- **Security Intelligence** (renseignements de sécurité) : Permettent de bloquer les mauvaises adresses IP et URL. Pour de plus amples renseignements, consultez la section Comment bloquer les menaces, à la page 56.

Remarque
Tout le trafic chiffré sur les interfaces passives est classé comme non déchiffrable, de sorte que les règles de déchiffrement SSL sont inefficaces et ne s'appliquent pas aux interfaces passives.

Étape 7 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Étape 8 Utilisez les tableaux de bord de surveillance pour analyser les types de trafic et les menaces qui traversent le réseau. Si vous décidez que vous souhaitez que le périphérique Firepower Threat Defense supprime activement les connexions indésirables, redéployez le périphérique afin de pouvoir configurer des interfaces de routage actives qui assurent la protection par pare-feu du réseau surveillé.

Plus d'exemples

En plus des exemples présentés dans le chapitre Use Case (Cas d'utilisation), il existe des exemples de configuration dans certains chapitres qui expliquent des services spécifiques. Les exemples suivants pourraient vous intéresser.

Contrôle d'accès

- Comment contrôler l'accès au réseau à l'aide des balises de groupe de sécurité TrustSec, à la page 532

Traduction d'adresses réseau (NAT)

NAT pour les adresses IPv4

- Fournir l'accès à un serveur Web interne (NAT automatique statique), à la page 622
- Adresse unique pour FTP, HTTP et SMTP (NAT automatique statique avec traduction de port), à la page 625
- Traduction différente selon la destination (PAT manuelle dynamique), à la page 631
- Traduction différente selon l'adresse et le port de destination (PAT manuelle dynamique), à la page 637
- Modification de la réponse DNS, serveur DNS externe, à la page 649

- Modification de la réponse DNS, serveur DNS sur le réseau hôte, à la page 652
- Exemption du trafic VPN de site à site de la NAT, à la page 685

NAT pour les adresses IPv6

- Exemple NAT64/46 : réseau IPv6 interne avec Internet IPv4 externe, à la page 608
- Exemple NAT64/46 : réseau interne IPv6 avec Internet IPv4 externe et traduction DNS, à la page 610
- Exemple NAT66, de traduction statique entre réseaux, à la page 615
- Exemple de NAT66, PAT d'interface IPv6 simple, à la page 618
- Modification de la réponse DNS64, à la page 643

Réseau privé virtuel d'accès à distance

- Comment mettre en œuvre la modification d'autorisation RADIUS, à la page 736
- Comment configurer l'authentification à deux facteurs à l'aide de Duo LDAP, à la page 745
- Comment fournir un accès Internet sur l'interface externe pour les utilisateurs du VPN d'accès à distance (Hair Pinning), à la page 752
- Comment utiliser un serveur de répertoire sur un réseau externe avec le VPN d'accès à distance, à la page 757
- Comment contrôler l'accès VPN RA par groupe, à la page 772
- Comment autoriser l'accès au VPN d'accès à distance aux réseaux internes dans différents routeurs virtuels., à la page 775
- Comment personnaliser l'icône et le logo client AnyConnect, à la page 779

Réseau privé virtuel site à site (VPN)

- Exemption du trafic VPN de site à site de la NAT, à la page 685
- Comment fournir un accès Internet sur l'interface externe pour les utilisateurs d'un VPN site à site externe (hairpinning), à la page 691
- Sécuriser le trafic de réseaux dans plusieurs routeurs virtuels sur un VPN de site à site, à la page 698

Déchiffrement SSL/TLS

- Exemple : blocage des anciennes versions SSL/TLS du réseau, à la page 470

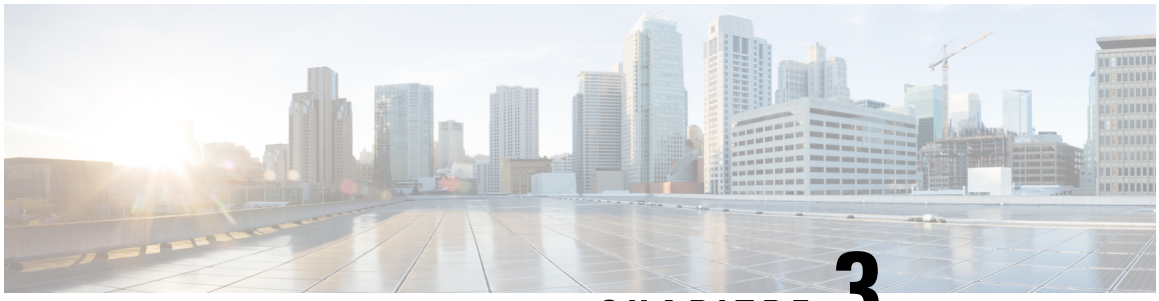
Politique FlexConfig

- Comment activer et désactiver les inspections globales par défaut, à la page 895
- Comment annuler vos modifications FlexConfig, à la page 900
- Comment activer les inspections pour les classes de trafic uniques, à la page 902

Routage virtuel

- Fournir un accès Internet à plusieurs routeurs virtuels avec des espaces d'adresses en chevauchement , à la page 347

- Comment effectuer un routage vers un serveur distant à l'aide de routeurs virtuels, à la page 342
- Comment autoriser l'accès au VPN d'accès à distance aux réseaux internes dans différents routeurs virtuels., à la page 775
- Sécuriser le trafic de réseaux dans plusieurs routeurs virtuels sur un VPN de site à site, à la page 698



CHAPITRE 3

Octroi de licence du système

Les rubriques suivantes expliquent comment obtenir une licence pour le périphérique Firewall Threat Defense.

- Licences Smart pour le système de pare-feu, à la page 87
- Gestion des licences Smart, à la page 92
- Application des licences permanentes, à la page 98

Licences Smart pour le système de pare-feu

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 logiciel n'est pas verrouillé par un nœud sur votre matériel, vous pouvez donc facilement utiliser et transférer des licences selon vos besoins.

Pour utiliser les licences Smart, vous devez d'abord configurer un compte Smart sur Cisco Software Central (software.cisco.com).

Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à cisco.com/go/licensingguide

Cisco Smart Software Manager

Lorsque vous achetez une ou plusieurs licences pour le périphérique Firewall Threat Defense, vous les gérez dans le Cisco Smart Software Manager : https://software.cisco.com/#SmartLicensing-Inventory. Le Cisco 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 principal. En tant qu'administrateur du compte, vous pouvez créer d'autres comptes virtuels. par exemple, pour les régions, les services ou les filiales. Plusieurs comptes virtuels vous aident à gérer un grand nombre de licences et de périphériques.

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.

Lorsque vous enregistrez un périphérique dans Cisco Smart Software Manager, vous créez un Product Instance Registration Token (jeton d'enregistrement d'instance de produit) dans le gestionnaire, puis vous le saisissez dans Gestionnaire de périphériques de pare-feu. Un périphérique enregistré est associé à un compte virtuel en fonction du jeton utilisé.

Pour en savoir plus sur le Cisco Smart Software Manager, consultez l'aide en ligne du gestionnaire.

Communication périodique avec l'autorité de licence

Lorsque vous utilisez un jeton d'enregistrement d'instance de produit pour enregistrer un Firewall Threat Defense, le périphérique s'enregistre auprès de l'autorité de licence de Cisco. L'autorité de licence délivre un certificat d'identification pour la communication entre le périphérique et l'autorité de licence. Ce certificat est valide pour un an, mais il sera renouvelé tous les six mois. Si un certificat d'identification expire (généralement au bout de neuf mois ou d'un an sans communication), le périphérique passe à l'état Non inscrit et l'utilisation des fonctionnalités sous licence est suspendue.

Le périphérique communique avec l'autorité de licence sur une base périodique. Si vous apportez des modifications dans Cisco 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. La communication normale de licence a lieu toutes les 12 heures, mais avec le délai de grâce, votre périphérique fonctionnera jusqu'à 90 jours sans appel à Cisco. Vous devez communiquer avec l'autorité de licence avant que les 90 jours ne soient écoulés.

Type de licence Smart

Le tableau suivant présente les licences disponibles pour le périphérique Firewall Threat Defense.

L'achat d'un périphériqueFirewall Threat Defense comprend automatiquement une licence De base. Toutes les licences supplémentaires sont facultatives.

Tableau 5 : Type de licence Smart

Licence	Durée	Capacités accordées
De base	Perpétuel	Toutes les fonctionnalités non couvertes par les licences à durée déterminée optionnelles. La licence De base est automatiquement ajoutée à votre compte lors de votre enregistrement. Vous devez préciser s'il faut permettre la fonction de contrôle de l'exportation sur les produits enregistrés avec ce jeton (**Allow export-controlled functionality on the products registered with this token**). Vous ne pouvez sélectionner cette option que si votre pays respecte les normes de contrôle des exportations. Cette option régit votre utilisation du chiffrement avancé et les fonctionnalités qui nécessitent un chiffrement avancé.

Licence	Durée	Capacités accordées
Menace	À durée déterminée	Nécessaire pour utiliser les politiques suivantes : • Intrusion • Fichier (le Programme malveillant est également requis) • Renseignements sur la sécurité
Programme malveillant	À durée déterminée	Politiques de fichiers (le Menace est également obligatoire).
URL	À durée déterminée	Politiques d'URL : filtrage d'URL basé sur la catégorie et la réputation ou filtrage des demandes de recherche DNS. Vous pouvez effectuer le filtrage d'URL sur des URL individuelles sans cette licence.
VPN d'accès à distance : • AnyConnect Plus • AnyConnect Apex • VPN AnyConnect	Licences à durée déterminée ou perpétuelle selon le type de licence.	Configuration VPN d'accès à distance Votre licence de base doit autoriser les fonctionnalités soumises à contrôle à l'exportation pour configurer le VPN d'accès à distance. Vous pouvez choisir de respecter ou non les exigences d'exportation lors de l'enregistrement du périphérique . Gestionnaire de périphériques de pare-feu peut utiliser n'importe quelle licence client AnyConnect valide. Les fonctionnalités disponibles ne varient pas selon le type de licence. Si vous n'en avez pas encore acheté, consultez Exigences de licence pour le VPN d'accès à distance, à la page 710. Voir aussi le *Guide de commande Cisco AnyConnect*, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf.

Obtention de licence pour Firewall Threat Defense Virtual

Cette section décrit les droits de licence par niveau de performance disponibles pour FTDv.

Toute licence FTDv peut être utilisée sur n'importe quelle configuration vCPU/mémoire FTDvprise en charge. Cela permet aux clients FTDv d'exécuter une grande variété d'empreintes de ressources de VM. Cela augmente également le nombre d'instances AWS et Azure prises en charge. Lors de la configuration de la machine virtuelle FTDv, le nombre maximal de cœurs (vCPU) pris en ; et la mémoire maximale prise en charge est de 32 Go .

Niveaux de performance pour Smart Licensing Firewall Threat Defense Virtual

Les limites de session pour les RA VPN sont déterminées par le niveau d'autorisation de la plateforme FTDv installée et appliquées par l'intermédiaire d'un limiteur de débit. Le tableau suivant récapitule les limites de session en fonction du niveau d'admissibilité et du limiteur de débit.

Tableau 6 : Firewall Threat Defense Virtual Limites des fonctionnalités sous licence en fonction des droits

Niveau de performance	Caractéristiques du périphérique (cœur/RAM)	Limite du débit	Limite de session RA VPN
FTDv5, 100 Mbit/s	4 cœurs/8 Go	100 Mbit/s	50
FTDv10, 1 Gbit/s	4 cœurs/8 Go	1 Gbit/s	250
FTDv20, 3 Gbit/s	4 cœurs/8 Go	3 Gbit/s	250
FTDv30, 5 Gbit/s	8 cœurs/16 Go	5 Gbit/s	250
FTDv50, 10 Gbit/s	12 cœurs/24 Go	10 Gbit/s	750
FTDv100, 16 Gbit/s	16 cœurs/32 Go	16 Gbit/s	10 000

Lignes directrices et limites des licences de niveaux de performanceFirewall Threat Defense Virtual

N'oubliez pas de tenir compte des consignes et restrictions suivantes lors de la mise sous licence de votre appareil FTDv.

- Le FTDv prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement.
- Toute licence FTDv peut être utilisée sur n'importe quelle configuration de cœur/mémoire FTDvprise en charge. Cela permet aux FTDv clients de fonctionner sur une grande variété de profils de ressources VM.
- Vous pouvez sélectionner un niveau de performance lorsque vous déployez le FTDv, que votre appareil soit en mode d'évaluation ou qu'il soit déjà enregistré auprès de Cisco Smart Software Manager.

Remarque Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin. Il est important de choisir le niveau qui correspond à la licence présente dans votre compte. Si vous mettez à niveau votre FTDv pour la version 7.0, vous pouvez choisir **FTDv - Variable** pour maintenir la conformité de votre licence actuelle. Votre FTDv continue de fonctionner avec des limites de session en fonction des capacités de votre appareil (nombre de cœurs/RAM).

- Le niveau de performance par défaut est FTDv50 lors du déploiement d'un nouvel appareil FTDv ou lors du provisionnement de FTDv à l'aide de l'API REST.
- Les licences De base sont basées sur un abonnement et sont mappées aux niveaux de performance. Votre compte virtuel doit disposer des droits de licence De base pour les périphériques FTDv, ainsi que des licences Menace , Programme malveillant, Filtrage d'URL.
- Chaque homologue de haute disponibilité (HA) correspond à un droit et les droits s'appliquant sur chaque homologue HA doivent correspondre, y compris la licence De base.
- Une modification du niveau de performance pour une paire haute disponibilité doit être appliquée à l'homologue principal.

- La licence Universal PLR est appliquée à chaque périphérique d'une paire haute disponibilité séparément. Le périphérique secondaire ne reflétera pas automatiquement le niveau de performance du périphérique principal. Il doit être mis à jour manuellement.

Incidence du paramètre de contrôle des exportations sur les fonctionnalités de chiffrement

Vous devez préciser s'il faut **Allow export-controlled functionality** (Autoriser les fonctionnalités soumises au contrôle des exportations). Vous ne pouvez sélectionner cette option que si votre pays respecte les normes de contrôle des exportations. Cette option régit votre utilisation du chiffrement avancé et les fonctionnalités qui nécessitent un chiffrement avancé.

Le mode d'évaluation est traité de la même manière que l'enregistrement à l'aide d'un compte non conforme à la norme d'exportation. Cela signifie que vous ne pouvez pas configurer le VPN d'accès à distance ou utiliser des algorithmes de chiffrement avancés lors de l'exécution en mode d'évaluation.

Plus particulièrement, la norme DES est disponible uniquement en mode d'évaluation ou non conforme à l'exportation.

Ainsi, si vous configurez des fonctionnalités chiffrées, telles que le VPN de site à site, ou si vous chiffrez la connexion de basculement dans un groupe à haute disponibilité, vous risquez de rencontrer des problèmes de connexion après vous être enregistré dans un compte conforme à l'exportation. Si la fonctionnalité utilisait DES en mode d'évaluation, cette configuration sera interrompue après l'enregistrement du compte.

Tenez compte des recommandations suivantes pour éviter les problèmes liés au chiffrement :

- Évitez de configurer des fonctionnalités chiffrées, telles que le VPN de site à site et les connexions de basculement chiffrées, avant d'avoir enregistré le périphérique.
- Après avoir enregistré le périphérique à l'aide d'un compte conforme à l'exportation, modifiez toutes les fonctionnalités de chiffrement que vous avez configurées en mode d'évaluation et sélectionnez des algorithmes de chiffrement plus sécurisés. Testez et vérifiez chacune de ces fonctionnalités pour vous assurer qu'elles fonctionnent correctement.



Remarque Si vous avez configuré le chiffrement de basculement à haute disponibilité en mode d'évaluation, vous devrez également redémarrer les deux périphériques du groupe à haute disponibilité pour commencer à utiliser un chiffrement plus fort. Nous vous recommandons de supprimer d'abord le chiffrement pour éviter une situation de split-brain, dans laquelle les deux périphériques se considèrent comme l'unité active.

Incidence des licences facultatives expirées ou désactivées

Si l'une des licences facultatives suivantes expire, vous pouvez continuer à utiliser les fonctionnalités qui nécessitent la licence. Cependant, la licence est marquée comme non conforme et vous devez l'acheter et l'ajouter à votre compte pour la rendre conforme.

Si vous désactivez une licence facultative, le système réagit comme suit :

- Programme malveillant—Le système cesse d'interroger le Cisco Secure Malware Analytics Cloud et cesse également d'accuser réception des événements rétrospectifs envoyés par le Cisco Secure Malware Analytics Cloud. Vous ne pouvez pas redéployer des stratégies de contrôle d'accès existantes si elles

comprennent des politiques de fichiers. Notez que, pendant un très court laps de temps après la désactivation d'une licence, le système peut utiliser les dispositions de fichiers en cache existantes.Programme malveillant À l'expiration de ce délai, le système attribue à ces fichiers la mention unavailable (Indisponible).

- Menace —Le système n'applique plus les politiques de prévention des intrusions ou de fichiers. Pour les politiques de renseignements de sécurité, le système n'applique plus la politique et arrête de télécharger les mises à jour de flux. Vous ne pouvez pas redéployer les politiques existantes qui nécessitent la licence.
- URL—Les règles de contrôle d'accès avec des conditions de catégorie d'URL arrêtent immédiatement de filtrer les URL ou les demandes de recherche DNS, et le système ne télécharge plus les mises à jour des données d'URL. Vous ne pouvez pas redéployer des politiques de contrôle d'accès existantes si elles comprennent des règles avec des conditions d'URL basées sur la catégorie et la réputation.
- RA VPN—Vous ne pouvez pas modifier la configuration du VPN d'accès à distance, mais vous pouvez la supprimer. Les utilisateurs peuvent toujours se connecter en utilisant la configuration VPN d'accès à distance. Toutefois, si vous modifiez l'enregistrement du périphérique de sorte que le système n'est plus conforme à la norme d'exportation, la configuration VPN d'accès à distance s'arrête immédiatement et aucun utilisateur distant ne peut se connecter par l'intermédiaire du VPN.

Gestion des licences Smart

Utilisez la page License Smart pour afficher l'état actuel de la licence pour le système. Le système doit être sous licence.

La page vous indique si vous utilisez la licence d'évaluation de 90 jours ou si vous vous êtes enregistré auprès de Cisco Smart Software Manager. Une fois enregistré, vous pouvez voir l'état de la connexion à Cisco Smart Software Manager ainsi que l'état de chaque type de licence.

L'autorisation d'utilisation identifie l'état de l'agent de License Smart :

- Authorized (Autorisé) (Connected (Connecté), Sufficient Licenses (Licences suffisantes)) : le périphérique a contacté et enregistré avec succès l'autorité de licence, qui a autorisé les droits de licence pour le périphérique. L'appareil est maintenant In-Compliance (conforme).
- Out-of-Compliance (Non conforme) : il n'y a aucun droit de licence disponible pour le périphérique. Les fonctionnalités sous licence continuent de fonctionner. Cependant, vous devez acheter ou libérer des licences supplémentaires pour être en conformité.
- Autorisation expirée (Authorization Expired) : l'appareil n'a pas communiqué avec l'autorité de licence depuis 90 jours ou plus. Les fonctionnalités sous licence continuent de fonctionner. Dans cet état, l'agent de License Smart relance ses demandes d'autorisation. Si une nouvelle tentative réussit, l'agent entre dans un état Out-of-Compliance (Non conforme) ou Authorized (Autorisé) et une nouvelle période d'autorisation commence. Essayez de synchroniser manuellement l'appareil.

Remarque Cliquez sur le bouton **i** à côté de l'état de la licence Smart pour afficher le compte virtuel, les fonctions à exportation contrôlée et obtenir un lien pour ouvrir le Cisco Smart Software Manager. Les fonctions à exportation contrôlée contrôlent les logiciels assujettis aux lois et règlements relatifs à la sécurité nationale, à la politique étrangère et à la prévention du terrorisme.

La procédure suivante fournit un aperçu de la gestion des licences pour le système.

Avant de commencer

Si vous n'avez pas de chemin d'accès à Internet pour le système, vous ne pouvez pas utiliser les licences Smart. Au lieu de cela, passez en mode Réservation de licence permanente (PLR). Pour de plus amples renseignements, voir Application des licences permanentes, à la page 98.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **Afficher la configuration** dans le résumé de la licence Smart.

Étape 2 Enregistrez l'appareil.

Vous devez vous inscrire auprès de Cisco Smart Software Manager avant de pouvoir attribuer les licences facultatives. Veuillez vous inscrire avant la fin de la période d'évaluation.

Consultez Enregistrement de l'appareil, à la page 93.

Remarque
Lors de votre enregistrement, vous choisissez d'envoyer ou non les données d'utilisation à Cisco. Vous pouvez modifier votre choix en cliquant sur le lien **Go To Cisco Success Network** (Accéder à Cisco Success Network) à côté de l'icône en forme d'engrenage.

Étape 3 Demandez et gérez les licences de fonctionnalités facultatives.

Vous devez activer une licence pour utiliser les fonctionnalités contrôlées par la licence. Consultez Activation ou désactivation des licences facultatives, à la page 95.

Étape 4 Maintenir l'octroi de licences système.

Vous pouvez effectuer les tâches suivantes :

- Synchronisation avec Cisco Smart Software Manager, à la page 96
- Désinscrire le périphérique, à la page 97

Enregistrement de l'appareil

Votre achat de l'appareil Firewall Threat Defense inclut automatiquement une licence De base. La licence De base englobe toutes les fonctionnalités non couvertes par les licences facultatives. C'est une licence permanente.

Lors de la configuration initiale du système, vous êtes invité à enregistrer le périphérique auprès de Cisco Smart Software Manager. Si vous avez plutôt choisi d'utiliser la licence d'évaluation de 90 jours, vous devez enregistrer l'appareil avant la fin de la période d'évaluation.

Lorsque vous enregistrez le périphérique, votre compte virtuel alloue la licence au périphérique. L'enregistrement de l'appareil permet également d'enregistrer toutes les licences facultatives que vous avez activées.

Avant de commencer

Lorsque vous enregistrez un périphérique, seul ce périphérique est enregistré. Si le périphérique est configuré pour la haute disponibilité, vous devez vous connecter à l'autre unité de la paire à haute disponibilité pour enregistrer cette unité.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Cliquez sur **Register Device (enregistrer l'appareil)** et suivez les instructions.

a) Cliquez sur le lien pour ouvrir Cisco Smart Software Manager et vous connecter à votre compte, ou en créer un si nécessaire.

b) Générer un nouveau jeton.

Lorsque vous créez le jeton, vous précisez la durée de validité du jeton. La période d'expiration recommandée est de 30 jours. Cette période définit la date d'expiration du jeton lui-même et n'a aucun impact sur le périphérique que vous enregistrez à l'aide du jeton. Si le jeton expire avant que vous puissiez l'utiliser, vous pouvez simplement générer un nouveau jeton.

Vous devez préciser s'il faut permettre la fonction de contrôle de l'exportation sur les produits enregistrés avec ce jeton (**Allow export-controlled functionality on the products registered with this token**). Vous ne pouvez sélectionner cette option que si votre pays respecte les normes de contrôle des exportations. Cette option régit votre utilisation du chiffrement avancé et les fonctionnalités qui nécessitent un chiffrement avancé.

c) Copiez et collez le jeton dans la zone d'édition de la boîte de dialogue Smart License Registration.

d) (**Firewall Threat Defense Virtual uniquement**) Sélectionnez un niveau de performance pour votre appareil FTDv ou laissez la sélection par défaut.

Lorsqu'aucun niveau de performance n'est sélectionné, votre appareil FTDv fonctionne en mode hérité avec des paramètres par défaut de 4 cœurs/8 Go; consultez Changer le niveau de performance Firewall Threat Defense Virtual, à la page 94 pour avoir plus d'informations.

e) Sélectionnez votre région pour l'enregistrement en lien avec les services en nuage Cisco.

Après l'enregistrement, si vous devez modifier cette région, vous devrez annuler l'enregistrement de l'appareil, puis l'enregistrer de nouveau et sélectionner la nouvelle région.

f) Décidez d'envoyer ou non les données d'utilisation à Cisco.

Lisez les informations à l'étape sur le Cisco Success Network (Réseau de succès Cisco), cliquez sur le lien **Sample Data** (échantillon de données) pour afficher les données réelles recueillies, puis décider si l'option **Enable Cisco Success Network** (activer le Réseau de succès Cisco) est activée.

g) Cliquez sur (demander l'enregistrement)**Register Device**(enregistrer l'appareil).

Changer le niveau de performance Firewall Threat Defense Virtual

Le FTDv prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement. Toute licence FTDv peut être utilisée

sur n'importe quelle configuration de cœur/mémoire FTDvprise en charge. Cela permet aux clients FTDv de fonctionner sur une grande variété d'empreintes de ressources VM ; voir Niveaux de performance pour Smart Licensing Firewall Threat Defense Virtual, à la page 89.

Lorsque vous effectuez une mise à niveau de FTDv vers la version 7.0 ou ultérieure, l'appareil passe automatiquement à l'état « FTDv Variable » et continue de consommer des droits non hiérarchisés jusqu'à ce que vous établissiez le niveau de droit.

Gardez les éléments suivants à l'esprit :

- Vous pouvez modifier le niveau de performance pour répondre à vos besoins de déploiement en fonction du débit ou des exigences de VPN RA. N'oubliez pas que FTDv se déploie avec des ressources de base et de mémoire ajustables. Le niveau de performance sélectionné ne doit pas dépasser les spécifications de votre appareil.
- La modification du niveau de performance n'est pas prise en charge pour AWS.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Sélectionnez l'option souhaitée dans la liste déroulante des niveaux de performance (**Performance Tier**).

- FTDv5 (4 cœurs/8 Go)
- FTDv10 (8 cœurs/8 Go)
- FTDv20 (8 cœurs/8 Go)
- FTDv30 (8 cœurs/16 Go)
- FTDv50 (12 cœurs/24 Go)
- FTDv100 (16 cœurs/24 Go)

Remarque
Le système met en évidence le niveau optimal en fonction des spécifications actuelles du périphérique.

Étape 3 Passez en revue votre sélection et les spécifications de l'appareil.

Remarque
Lors de la configuration de la machine virtuelle FTDv, le nombre maximal de cœurs (vCPU) pris en charge est de 12 (16 pour FTDv100 sur VMware et KVM); et la mémoire maximale prise en charge est de 24 Go de RAM. Le niveau de performance sélectionné ne doit pas dépasser les spécifications de votre appareil.

Étape 4 Cliquez sur **YES** (oui) pour modifier le niveau de performance.

Activation ou désactivation des licences facultatives

Vous pouvez activer (enregistrer) ou désactiver (libérer) les licences facultatives. Vous devez activer une licence pour utiliser les fonctionnalités contrôlées par la licence.

Si vous ne souhaitez plus utiliser les fonctionnalités couvertes par une licence facultative, vous pouvez désactiver celle-ci. La désactivation de la licence la libère dans votre compte Cisco Smart Software Manager. Vous pourrez ensuite appliquer cette licence à un autre appareil.

Vous pouvez également activer les versions d'évaluation de ces licences lors de leur exécution en mode d'évaluation. En mode d'évaluation, les licences ne sont enregistrées auprès de Cisco Smart Software Manager que lorsque vous enregistrez le périphérique. Cependant, vous ne pouvez pas activer la licence VPN d'accès à distance ou en mode d'évaluation.

Avant de commencer

Avant de désactiver une licence, vérifiez que vous ne l'utilisez pas. Procédez à la réécriture ou à la suppression de toutes les politiques nécessitant la licence.

Pour les unités fonctionnant selon une configuration à haute disponibilité, vous activez ou désactivez les licences sur l'unité active uniquement. La modification se répercute sur l'unité de secours lors du prochain déploiement de la configuration, lorsque l'unité de secours demande (ou libère) les licences nécessaires. Lorsque vous activez des licences, vous devez vous assurer que votre compte Cisco Smart Software Manager dispose de suffisamment de licences, sinon vous pourriez vous retrouver avec une unité conforme alors que l'autre unité est non conforme.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Cliquez sur **Enable/Disable** (activer/désactiver) pour chaque licence facultative, au besoin.

- **Enable** (activer) : Enregistre la licence avec votre compte Cisco Smart Software Manager et active les fonctionnalités contrôlées. Vous pouvez maintenant configurer et déployer les politiques contrôlées par la licence.
- **Disable** (désactiver) : Désinscrit la licence de votre compte Cisco Smart Software Manager et désactive les fonctionnalités contrôlées. Vous ne pouvez ni configurer les fonctionnalités dans de nouvelles politiques, ni déployer des politiques qui utilisent les fonctionnalités.

Étape 3 Si vous avez activé la licence **RA VPN**, sélectionnez le type de licence disponible dans votre compte.

Vous pouvez utiliser n'importe quelle licence client AnyConnect : **Plus**, **Apex**, ou **VPN Only**. Vous pouvez sélectionner **Plus et Apex** si vous avez les deux licences et que vous souhaitez les utiliser.

Synchronisation avec Cisco Smart Software Manager

Le système synchronise périodiquement les informations de licence avec Cisco Smart Software Manager. La communication normale de licence a lieu tous les 30 jours, mais avec le délai de grâce, votre appareil fonctionnera jusqu'à 90 jours sans appel à Cisco.

Si vous apportez des modifications dans Cisco Smart Software Manager, vous pouvez actualiser l'autorisation sur le périphérique pour que les modifications prennent effet immédiatement.

La synchronisation obtient l'état actuel des licences et renouvelle l'autorisation et le certificat d'ID.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **Afficher la configuration** dans le résumé de la licence Smart.

Étape 2 Sélectionnez **Resync Connection** (Resynchroniser la connexion) dans la liste déroulante d'engrenage.

Désinscrire le périphérique

Si vous ne souhaitez plus utiliser le périphérique, vous pouvez le désinscrire du gestionnaire de logiciels Cisco Smart. Lorsque vous vous désinscrirez, la licence De base de base et toutes les licences facultatives associées au périphérique sont libérées dans votre compte virtuel. Des licences facultatives peuvent être attribuées à d'autres périphériques. En outre, l'appareil n'est pas enregistré pour Cisco Cloud et Cisco Cloud Services.

Après la désinscription du dispositif, la configuration et les politiques actuelles sur le dispositif continuent de fonctionner telles quelles, mais vous ne pouvez pas apporter de modifications ou déployer des modifications.



Mise en garde Vous devez utiliser cette procédure pour annuler l'enregistrement de l'appareil. Si vous vous désinscrivez plutôt de votre compte Cisco Smart Software Manager, il y aura une incohérence entre l'état de la licence sur le périphérique et celui dans Cisco Smart Software Manager. Cela entraînera des erreurs lorsque vous tenterez de nouveau de fournir une licence à l'appareil, par exemple lorsque vous formerez une paire à haute disponibilité. Les messages symptômes de cette défaillance sont « Échec de génération de jeton pour s'inscrire auprès de Cisco Cloud au moyen d'une licence Smart » et « Impossible de retourner le certificat pour le NS donné (*numéro de série*) car il est REMIS À NEUF . » Si cela se produit, annulez l'enregistrement des unités en utilisant cette procédure et réessayez.

Avant de commencer

Lorsque vous annulez l'enregistrement d'un périphérique, seul cet appareil est désinscrit. Si l'appareil est configuré pour la haute disponibilité, vous devez vous connecter à l'autre appareil de la paire de haute disponibilité pour désinscrire cet appareil.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Sélectionnez **Unregistrer Device (désinscrire l'appareil)** dans la liste déroulante en forme d'engrenage.

Étape 3 Lisez l'avertissement et cliquez sur **Unregister (annuler l'enregistrement)** si vous souhaitez vraiment annuler l'enregistrement du périphérique.

Application des licences permanentes

Vous pouvez appliquer des licences permanentes dans les réseaux non isolés et isolés. Un réseau isolé est un réseau dans lequel il n'y a pas de chemin d'accès à l'Internet. Il s'agit de réseaux à haute sécurité où vous souhaitez empêcher toute possibilité d'intrusion et d'attaque depuis l'extérieur. Comme il n'y a aucun accès à Internet, vous ne pouvez pas enregistrer le périphérique directement auprès de Cisco Smart Software Manager. Vous pouvez plutôt utiliser le mode Permanent License Reservation (PLR) (réservation de licence permanente) pour obtenir une licence que vous pourrez appliquer au périphérique.

Si vous devez utiliser le mode PLR, gardez les points suivants à l'esprit :

- Les fonctionnalités qui nécessitent un accès à Internet, comme les politiques de fichiers, les recherches d'URL ou le lancement contextuel vers des sites Web publics, ne fonctionneront pas.
- Même si vous activez Web Analytics et Cisco Success Network, Cisco ne collecte pas les données associées, faute d'accès à Internet.
- Vous devrez charger manuellement les mises à jour de la base de données de géolocalisation, des règles de prévention des intrusions et de la base de données des vulnérabilités (VDB). Par exemple, vous pouvez télécharger les mises à jour sur une clé USB, puis l'apporter dans votre bâtiment sécurisé et les téléverser à partir d'un poste de travail sécurisé.



Remarque Cisco Smart Software Manager utilise le numéro de série du périphérique pour attribuer la licence permanente. Si vous devez désenregistrer le périphérique et que les processus habituels de désenregistrement ou d'annulation ne parviennent pas à supprimer l'attribution de licence, vous devrez communiquer avec l'assistance technique Cisco pour retirer l'enregistrement de Cisco Smart Software Manager. Le fait de réimager le périphérique ne supprimera pas l'enregistrement de la licence.

Les rubriques suivantes expliquent plus en détail les différents types de licences permanentes, la façon de les appliquer et comment annuler l'inscription ou désenregistrer le périphérique.

Réservation de licence permanente universelle et réservation de licence spécifique

Il existe deux types distincts de réservation de licence :

- Réservation de licence permanente universelle (Universal PLR ou UPLR) : la licence permanente universelle permet une utilisation perpétuelle et illimitée des produits de pare-feu pris en charge, y compris toutes les licences facultatives. Une fois que vous avez acheté et appliqué une licence permanente universelle, toutes les licences de fonctionnalités appliquées, qui sont normalement basées sur le temps, sont applicables de manière permanente. Cependant, vous êtes toujours responsable de l'achat des licences de remplacement à mesure qu'elles expirent dans votre compte de licences Smart. ISA 3000 ne prend pas en charge le mode Universal PLR.
- La réservation de licences spécifiques nécessite le même nombre et les mêmes types de licences que l'octroi de licences Smart standard. Lorsque vous obtenez cette licence, vous sélectionnez les licences de fonctionnalités facultatives que vous souhaitez en plus de la licence de base. Vous devez mettre périodiquement vos licences à jour à mesure qu'elles expirent.

Gestionnaire de périphériques de pare-feu prend en charge uniquement Universal PLR (PLR universel).

Vous devez travailler avec votre représentant Cisco pour activer le mode de réservation de licences permanentes universelles (PLR) dans votre compte Cisco Smart Software Manager (CSSM).

Vérifier que votre compte Smart peut fournir une licence universelle

Pour vérifier que vous pouvez obtenir et appliquer une licence permanente, connectez-vous à votre compte CSSM et accédez à la page **Smart Software Licensing (Licences logicielles Smart)** > **Inventory (Inventaire)**, puis cliquez sur l'onglet **Licences**. Si le bouton **License Reservation** (Réservation de licence) est affiché, vous êtes autorisé à obtenir des réservations de licence permanentes.

Cependant, ce bouton démarre un assistant qui fonctionne à la fois pour les licences universelles et spécifiques.

Vous devez également consulter votre liste de licences disponibles pour vérifier qu'il existe une licence universelle pour le périphérique. Cette licence s'affichera en tant qu'élément pouvant être sélectionné à l'étape 2 de l'assistant lancé par le bouton **License Reservation** (Réservation de licence).

Si le bouton **License Reservation** (Réservation de licence) est affiché et que vous pouvez obtenir une licence universelle, vous pouvez procéder à la conversion du système pour utiliser une licence permanente. Si le bouton ne s'affiche pas, ou si vous ne pouvez réserver que des licences spécifiques, communiquez avec votre représentant Cisco et demandez l'activation du mode Universal PLR (PLR universel) pour votre compte.

Passer en mode PLR et appliquer une licence universelle

Une fois que vous avez vérifié que vous pouvez obtenir une licence permanente, comme expliqué dans la section Vérifier que votre compte Smart peut fournir une licence universelle, à la page 99, et que vous avez acheté la licence universelle requise, vous pouvez passer en mode de réservation de licence permanente (PLR) et appliquer la licence.

Mise en garde Si vous êtes actuellement en mode d'évaluation, une fois que vous êtes passé en mode PLR, vous ne pouvez pas revenir au mode d'évaluation.

Avant de commencer

Si le périphérique est configuré pour la haute disponibilité, vous devez effectuer cette tâche séparément pour les deux périphériques du groupe à haute disponibilité.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis cliquez sur **View Configuration** (Afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Si vous avez déjà enregistré le périphérique à l'aide des licences Smart, sélectionnez **Unregister Device** (Annuler l'enregistrement du périphérique) dans la liste déroulante de l'icône d'engrenage, puis confirmez l'annulation de l'enregistrement. Attendez que la tâche de désenregistrement soit terminée avant de continuer.

Étape 3 Sélectionnez **Switch to Universal PLR** (Passer au PLR universel) dans la liste déroulante de l'icône d'engrenage pour passer au mode Universal Permanent License Reservation (PLR) (Réservation de licence permanente universelle).

Lisez l'avertissement et cliquez sur **Yes** (Oui) pour confirmer le changement.

Le système se convertit en mode PLR, puis démarre le processus d'enregistrement PLR.

Étape 4 Complétez l'inscription PLR.

a) Lorsque le système ouvre la boîte de dialogue Universal Permanent License Reservation (Réservation de licence permanente universelle), la première étape affiche le code de demande requis. Vous pouvez cliquer sur **Save As TXT** (Enregistrer sous TXT) pour l'enregistrer dans un fichier texte ou sur **Print** (Imprimer) pour l'imprimer. Vous pouvez également mettre en surbrillance la chaîne et appuyer sur Ctrl+C pour la copier dans le presse-papiers.

Si vous avez annulé le processus après avoir changé de mode, vous pouvez le reprendre à cette étape en cliquant sur **Continue Reservation** (Continuer la réservation) sur la page Licensing (Licences).

b) Connectez-vous à votre compte CSSM, accédez à la page **Smart Software Licensing** > **Inventory (Inventaire)**, puis cliquez sur l'onglet **Licences**.

c) Cliquez sur le bouton **License Reservation (Réservation de licence)** et suivez les instructions de l'assistant. Vous serez invité à saisir le code de demande que vous avez généré et, en retour, vous obtiendrez un code d'autorisation.

L'assistant comprend les étapes suivantes :

1. Saisissez le code de demande de licence, ou chargez le fichier texte qui contient ce code, puis cliquez sur **Next** (Suivant).
2. À l'étape 2, vous verrez les détails du produit pour le système auquel vous octroyez une licence et une liste à puces des licences disponibles. Sélectionnez la licence universelle pour un périphérique Firewall Threat Defense géré localement, puis cliquez sur **Next** (Suivant).
3. À l'étape 3, vérifiez que la bonne licence est sélectionnée, puis cliquez sur **Generate Authorization Code** (Générer le code d'autorisation).
4. À l'étape 4, vous verrez le code d'autorisation. Cliquez sur **Download as File** (Télécharger en tant que fichier) ou **Copy to Clipboard** (Copier dans le presse-papiers), le cas échéant, pour enregistrer le code.
5. Cliquez sur **Close** (Fermer) pour quitter l'assistant.

d) De retour dans le Gestionnaire de périphériques de pare-feu, collez le code d'autorisation dans le champ approprié.

Un code d'autorisation valide pour une licence universelle doit suivre le format suivant : XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXX, où X représente un caractère alphanumérique. Si votre code d'autorisation est plutôt un fichier XML, vous disposez d'une licence spécifique et vous ne pouvez pas l'utiliser sur ce système. Veuillez annuler l'enregistrement comme décrit dans Annuler l'enregistrement PLR, à la page 101, en vous assurant de libérer les licences réservées dans CSSM. Ensuite, faites appel à votre représentant Cisco pour convertir votre compte Smart au format PLR universel.

e) Cliquez sur **Register** (Enregistrer).

Le système commencera le processus d'enregistrement. Actualisez la page de licence pour vérifier l'état de l'enregistrement.

Étape 5 Activez les licences de fonctionnalités facultatives selon les besoins.

La licence universelle enregistre le périphérique pour la licence De base uniquement. Vous pouvez maintenant cliquer sur **Enable** (Activer) pour chacune des licences de fonctionnalité dont vous avez besoin.

Annuler l'enregistrement PLR

Vous pouvez annuler une demande de réservation de licence permanente universelle (PLR) avant qu'elle ne soit terminée. Par exemple, si vous démarrez le processus d'enregistrement PLR et découvrez que votre compte Smart Software Manager n'est pas configuré pour le PLR, vous pouvez annuler le processus pendant que vous obtenez l'autorisation pour le mode PLR et que votre compte de licence Smart est configuré correctement.

Si vous avez terminé le processus d'enregistrement PLR, vous ne pouvez pas l'annuler. Au lieu de cela, consultez Annuler l'enregistrement du périphérique en mode PLR, à la page 102.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le résumé de la licence Smart.

Étape 2 Sélectionnez **Cancel PLR** (Annuler le PLR) dans la liste déroulante pour lancer le processus d'annulation.

Étape 3 Sélectionnez l'option qui s'applique à votre situation:

- **J'ai une licence dans CSSM** : utilisez cette option si vous êtes passé par l'assistant d'enregistrement de licences dans Cisco Smart Software Manager (CSSM) et que vous avez obtenu un code d'autorisation. À ce stade, des licences sont réservées dans CSSM et vous devez les libérer.
- **Je n'ai pas de licence dans CSSM** : utilisez cette option si vous n'avez pas terminé l'assistant CSSM jusqu'au point où vous avez obtenu un code d'autorisation. Par exemple, si vous avez commencé l'enregistrement PLR dans Gestionnaire de périphériques de pare-feu, mais avez ensuite découvert que le bouton **de réservation de licence** n'était pas disponible dans votre compte Smart.

Étape 4 (Si vous avez sélectionné **J'ai une licence dans CSSM**.) Vous devez obtenir un code de version du CSSM pour vous assurer que vos licences ne sont plus marquées comme en cours d'utilisation. Sinon, ces licences ne seront pas utilisables par d'autres périphériques.

a) Collez le code d'autorisation que vous avez obtenu du CSSM (lors de l'enregistrement) dans la boîte de dialogue d'annulation, puis cliquez sur **Generate Release Code** (Générer le code de version).

b) Lorsqu'il y a un code dans le champ **Release License Code** (Code de licence de version), cliquez sur **Save As TXT** (Enregistrer en tant que TXT) pour l'enregistrer dans un fichier texte ou **Print** (Imprimer) pour l'impression. Vous pouvez également sélectionner le code et appuyer sur Ctrl+C pour le copier dans le presse-papiers.

c) Dans CSSM, recherchez le périphérique dans la page **Smart Software Licensing (Licences logicielles Smart)** > **Inventory (Inventaire)** (le nom est le numéro de série du périphérique), cliquez sur **Action** > **Remove (Retirer)**, et saisissez le code de version.

Attendez que le CSSM indique que le produit a été retiré avec succès.

Étape 5 Cliquez sur **OK** pour terminer le processus d'annulation.

Le système revient au mode de licence Smart. Cependant, l'enregistrement du périphérique sera annulé et vous ne pourrez pas redémarrer le mode d'évaluation. À ce stade, vous devez enregistrer le périphérique à l'aide d'une licence Smart ou passer au mode PLR et vous enregistrer de nouveau pour l'utiliser.

Annuler l'enregistrement du périphérique en mode PLR

Si vous n'avez plus besoin d'obtenir la licence du périphérique, par exemple, parce que vous le désactivez ou le déplacez vers une autre installation, où vous lui accorderez une licence séparément, vous pouvez annuler l'enregistrement du périphérique.

L'annulation de l'enregistrement du périphérique ramène la licence à un état inutilisé. Si vous n'annulez pas l'enregistrement du périphérique, la licence reste marquée comme en cours d'utilisation et vous ne pouvez pas l'utiliser à d'autres fins.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le résumé Smart License (Licence Smart).

Étape 2 Sélectionnez **Unregister Universal PLR** (Annuler l'enregistrement d'un PLR universel) dans la liste déroulante , lisez l'avertissement et cliquez sur **Yes** (oui) pour lancer le processus.

Étape 3 Lorsque la boîte de dialogue Unregister Universal Permanent License Reservation (Annuler l'enregistrement de la licence permanente universelle) s'ouvre, le champ **Release License Code** (Libérer le code de licence) est rempli avec le code dont vous avez besoin pour libérer les licences actuellement attribuées dans votre compte CSSM. Cliquez sur **Save as TXT** (Enregistrer en tant que TXT) ou **Print** (Imprimer) pour conserver une copie de ce code. Vous pouvez également le sélectionner et utiliser les touches Ctrl+C pour le copier dans le presse-papiers.

Étape 4 Accédez à votre compte CSSM, recherchez le périphérique dans la page **Smart Software Licensing (Licences logicielles Smart)** > **Inventory (Inventaire)** (le nom est le numéro de série du périphérique), cliquez sur **Action** > **Remove (Retirer)**, et saisissez le code de version.

Attendez que le CSSM indique que le produit a été retiré avec succès.

Étape 5 De retour dans Gestionnaire de périphériques de pare-feu, cliquez sur **Unregister** (Annuler l'enregistrement) dans la boîte de dialogue Unregister Device (Annuler l'enregistrement du périphérique).

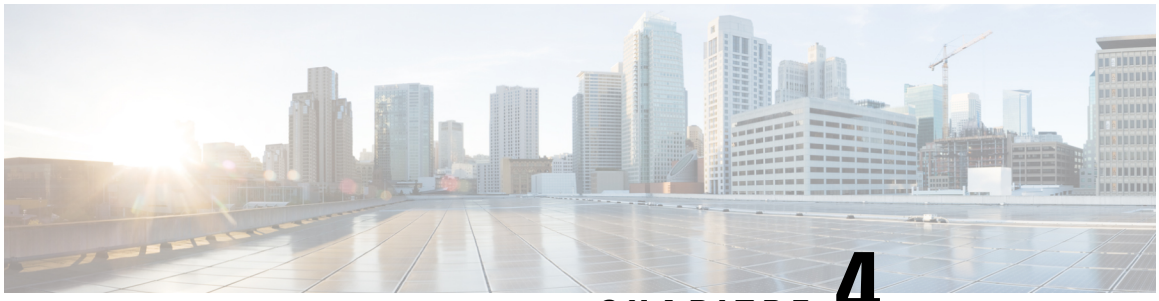
Cela termine le processus. À ce stade, les licences dans CSSM sont libres d'attribuer à un autre périphérique, et le périphérique Firewall Threat Defense n'est pas sous licence.



PARTIE I

Surveillance du système

- Surveillance du périphérique, à la page 105
- Alarmes pour Cisco ISA 3000, à la page 127



CHAPITRE 4

Surveillance du périphérique

Le système comprend des tableaux de bord et Event Viewer (la Visionneuse d'événements) que vous pouvez utiliser pour surveiller le périphérique et le trafic qui passe par le périphérique.

- Activer la journalisation pour obtenir des statistiques de trafic., à la page 105
- Tableaux de bord du trafic et du système, à la page 108
- Surveillance de statistiques supplémentaires à l'aide de l'interface de ligne de commande, à la page 112
- Affichage des événements, à la page 112

Activer la journalisation pour obtenir des statistiques de trafic.

Vous pouvez surveiller un large éventail de statistiques de trafic à l'aide des tableaux de bord de surveillance et de la visionneuse d'événements. Cependant, vous devez activer la journalisation pour indiquer au système quelles statistiques collecter. La journalisation génère différents types d'événements offrant une visibilité sur les connexions qui transitent par le système.

Les rubriques suivantes expliquent plus en détail les événements et les informations qu'ils fournissent, en se concentrant particulièrement sur la journalisation des connexions.

Types d'événements

Le système peut générer les types d'événements suivants. Vous devez générer ces événements pour voir les statistiques associées dans les tableaux de bord de surveillance.

Événements de connexion

Vous pouvez générer des événements pour les connexions car les utilisateurs génèrent du trafic qui traverse le système. Activez la journalisation de la connexion sur les règles d'accès pour générer ces événements. Vous pouvez également activer la journalisation sur les politiques de Security Intelligence et les règles de déchiffrement SSL pour générer des événements de connexion.

Les événements de connexion comprennent une grande variété d'informations sur une connexion, notamment les adresses IP et les ports source et de destination, les URL et les applications utilisées, ainsi que le nombre d'octets ou de paquets transmis. Les renseignements comprennent également l'action entreprise (par exemple, autoriser ou bloquer la connexion) et les politiques appliquées à la connexion.

Incidents d'intrusion

Le système examine les paquets qui traversent votre réseau pour détecter toute activité malveillante qui pourrait nuire à la disponibilité, à l'intégrité et à la confidentialité d'un hôte et de ses données. Lorsque

le système détecte une intrusion possible, il génère un incident d'intrusion, qui enregistre la date, l'heure, le type d'exploitation et des informations contextuelles sur la source de l'attaque et sa cible. Des incidents d'intrusion sont générés pour toute règle de prévention des intrusions définie pour bloquer ou alerter, quelle que soit la configuration de journalisation de la règle de contrôle d'accès à l'origine de l'invocation.

Événements liés aux fichiers

Les événements de fichier représentent les fichiers que le système a détectés, et éventuellement bloqués, dans le trafic réseau en fonction de vos politiques de fichiers. Vous devez activer la journalisation des fichiers sur la règle d'accès qui applique la politique de fichiers pour générer ces événements.

Lorsque le système génère un événement de fichier, le système consigne également la fin de la connexion associée, quelle que soit la configuration de journalisation de la règle de contrôle d'accès qui appelle.

Événements de maliciels

Le système peut détecter les programmes malveillants dans le trafic réseau dans le cadre de la configuration globale de votre contrôle d'accès. AMP for Firepower peut générer un événement de logiciel malveillant, contenant le statut de l'événement résultant et des données contextuelles indiquant comment, où et quand le logiciel malveillant a été détecté. Défense contre les programmes malveillants Vous devez activer la journalisation des fichiers sur la règle d'accès qui applique la politique de fichiers pour générer ces événements.

La disposition d'un fichier peut changer, par exemple, de « nettoyer » à malveillant ou d'un fichier malveillant à « nettoyer ». Si AMP for Firepower interroge le nuage AMP au sujet d'un fichier et que le nuage détermine que le statut a changé dans la semaine suivant la requête, le système génère des événements rétrospectifs de logiciel malveillant. Défense contre les programmes malveillantsCisco AMP Cloud

Événements liés aux renseignements sur la sécurité

Les événements Security Intelligence sont un type d'événement de connexion généré par la politique Security Intelligence pour chaque connexion bloquée ou surveillée par la politique. Tous les événements Security Intelligence comportent un champ Catégorie de Security Intelligence renseigné.

À chacun de ces événements correspond un événement de connexion « régulière ». Comme la politique de renseignements sur la sécurité est évaluée avant de nombreuses autres politiques de sécurité, y compris le contrôle d'accès, lorsqu'une connexion est bloquée par les renseignements sur la sécurité, l'événement qui en résulte ne contient pas les renseignements que le système aurait pu recueillir lors d'une évaluation ultérieure, par exemple, l'identité de l'utilisateur.

Journalisation des connexions configurable

Vous devez enregistrer les connexions en fonction des besoins de sécurité et de conformité de votre entreprise. Si votre objectif est de limiter le nombre d'événements que vous générez et d'améliorer les rendements, activez la journalisation uniquement pour les connexions essentielles à votre analyse. Toutefois, si vous souhaitez obtenir une vue d'ensemble de votre trafic réseau à des fins de profilage, vous pouvez activer la journalisation pour des connexions supplémentaires.

Lors de la configuration de la journalisation des connexions, gardez à l'esprit que le système peut journaliser une connexion pour plusieurs raisons et que la désactivation de la journalisation à un endroit ne garantit pas que les connexions correspondantes ne seront pas journalisées.

Vous pouvez configurer la journalisation des connexions aux emplacements suivants.

- Règles de contrôle d'accès et action par défaut : la journalisation à la fin d'une connexion fournit la plupart des informations sur la connexion. Vous pouvez aussi journaliser le début de la connexion, mais

ces événements comportent des informations incomplètes. La journalisation des connexions est désactivée par défaut; vous devez donc l'activer pour chaque règle (et l'action par défaut) qui cible le trafic que vous souhaitez suivre.

- ecurity Intelligence policy (Politique Security Intelligence) : vous pouvez activer la journalisation afin de générer des événements de connexion Security Intelligence pour chaque connexion bloquée. Lorsque le système journalise un événement de connexion à la suite du filtrage Security Intelligence, il journalise aussi un événement Security Intelligence correspondant, qui est un type particulier d'événement de connexion que vous pouvez afficher et analyser séparément.
- Règles de déchiffrement SSL et action par défaut : vous pouvez configurer la journalisation à la fin d'une connexion. Dans le cas des connexions bloquées, le système met immédiatement fin à la session et génère un événement. Pour les connexions surveillées et les connexions que vous transmettez aux règles de contrôle d'accès, le système génère un événement à la fin de la session.

Journalisation automatique des connexions

Le système enregistre automatiquement les événements de fin de connexion suivants, indépendamment de toute autre configuration de journalisation.

- Le système consigne automatiquement les connexions associées aux incidents d'intrusion, sauf si la connexion est gérée par l'action par défaut de la politique de contrôle d'accès. Vous devez activer la journalisation sur l'action par défaut pour obtenir les événements d'intrusion pour le trafic correspondant.
- Le système consigne automatiquement les connexions associées aux événements liés aux fichiers et aux programmes malveillants. Il s'agit uniquement des événements de connexion : vous pouvez éventuellement désactiver la génération d'événements liés aux fichiers et aux programmes malveillants.

Conseils pour la journalisation des connexions

Gardez les conseils suivants à l'esprit lors de l'examen de la configuration de votre journalisation et de l'évaluation des statistiques connexes :

- Lorsque vous autorisez le trafic avec une règle de contrôle d'accès, vous pouvez utiliser une politique de prévention des intrusions ou de fichiers associée pour inspecter davantage le trafic et bloquer les intrusions, les fichiers interdits et les programmes malveillants avant que le trafic n'atteigne sa destination finale. Notez, cependant, que l'inspection par défaut des fichiers et des intrusions est désactivée pour les charges utiles chiffrées. Si les politiques de prévention des intrusions ou de fichiers trouvent une raison de bloquer une connexion, le système consigne immédiatement un événement de fin de connexion, quels que soient vos paramètres de journal de connexion. La journalisation des connexions autorisées fournit la plupart des informations statistiques sur le trafic dans votre réseau.
- Une connexion de confiance est une connexion gérée par une règle de contrôle d'accès Trust (confiance) ou l'action par défaut dans une politique de contrôle d'accès. Cependant, les connexions de confiance ne sont pas inspectées pour détecter les données de découverte, les intrusions ou les fichiers interdits et les programmes malveillants. Par conséquent, les événements de connexion pour les connexions de confiance contiennent des informations limitées.
- Pour les règles de contrôle d'accès et les actions par défaut de la politique de contrôle d'accès qui bloquent le trafic, le système consigne les événements de début de connexion. Le trafic correspondant est refusé sans autre inspection.

- La journalisation des connexions TCP bloquées lors d'une attaque par déni de service (DoS) peut affecter le rendement du système et submerger la base de données avec plusieurs événements similaires. Avant d'activer la consignation pour une règle Block (Bloquer), évaluez si la règle surveille le trafic sur une interface exposée à Internet ou une autre interface vulnérable aux attaques DoS.
- Si vous sélectionnez l'option **Bypass Access Control policy for decrypted traffic** (Politique de contournement du contrôle d'accès pour le trafic déchiffré) (sysopt permit-vpn) lorsque vous configurez les profils de connexion VPN d'accès à distance, ou si vous activez la commande **sysopt connection permit-vpn**, tout le trafic de VPN de site à site ou d'accès à distance contourne l'inspection et la politique de contrôle d'accès. Ainsi, vous n'obtiendrez aucun événement de connexion pour ce trafic, et le trafic ne sera reflété dans aucun tableau de bord statistique.

Envoi d'événements à un serveur Syslog externe

Outre l'affichage des événements par le biais de Gestionnaire de périphériques de pare-feu, qui a une capacité limitée de stockage des événements, vous pouvez configurer de manière sélective les règles et les politiques pour envoyer des événements à un serveur syslog externe. Vous pouvez ensuite utiliser les fonctionnalités et le stockage supplémentaire de la plateforme de serveur syslog sélectionnée pour afficher et analyser les données d'événement.

Pour envoyer des événements à un serveur syslog externe, modifiez chaque règle, action par défaut ou politique qui active la journalisation des connexions et sélectionnez un objet serveur syslog dans les paramètres de journalisation. Pour envoyer des incidents d'intrusion à un serveur syslog, configurez le serveur dans les paramètres de la politique de prévention des intrusions. Pour envoyer des événements de fichier ou de programme malveillant à un serveur syslog, configurez le serveur dans **Device (Appareil)** > **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation**.

Pour en savoir plus, consultez l'aide de chaque type de règle et de politique, ainsi que Configuration des serveurs Syslog, à la page 154.

Évaluation des événements à l'aide des services en nuage Cisco

En plus d'utiliser Event Viewer (Visionneuse d'événements) et vos propres serveurs syslog, vous pouvez envoyer des événements de connexion ainsi que des événements d'intrusion prioritaires, de fichiers et de programmes malveillants à un serveur Cisco en nuage. Les services en nuage de Cisco, tels que Cisco Threat Response, peuvent extraire les événements de ce serveur en nuage et vous pouvez ensuite utiliser ces services pour évaluer ces événements.

Ces services en nuage sont distincts de l'appareil Firepower Threat Defenseet Gestionnaire de périphériques de pare-feu. Si vous choisissez d'utiliser un service qui vous oblige à envoyer ces événements dans le nuage Cisco, vous devez activer la connexion sur la page **Device (appareil)** > **System System Settings (Paramètres système** > **Cloud Services (Services en nuage)**. Consultez Envoi d'événements à Cisco Cloud, à la page 812.

Tableaux de bord du trafic et du système

Le système comprend plusieurs tableaux de bord que vous pouvez utiliser pour analyser le trafic passant par le périphérique et les résultats de votre politique de sécurité. Utilisez ces renseignements pour évaluer l'efficacité globale de votre configuration et pour identifier et résoudre les problèmes de réseau.

Les tableaux de bord des unités d'un groupe de haute disponibilité affichent les statistiques pour ce périphérique uniquement. Les statistiques ne sont pas synchronisées entre les unités.



Remarque Les données utilisées dans les tableaux de bord liés au trafic sont collectées à partir des règles de contrôle d'accès qui permettent la connexion ou de la journalisation des fichiers, et d'autres politiques de sécurité qui permettent la journalisation. Les tableaux de bord ne reflètent pas le trafic qui correspond aux règles pour lesquelles aucune journalisation n'est activée. Assurez-vous de configurer vos règles avec les informations qui vous intéressent. En outre, les renseignements sur les utilisateurs sont disponibles uniquement si vous configurez des règles d'identité pour recueillir l'identité des utilisateurs. Enfin, les informations sur les intrusions, les fichiers, les programmes malveillants et les catégories d'URL ne sont disponibles que si vous avez une licence pour ces fonctionnalités et si vous configurez les règles qui utilisent les fonctionnalités.

Procédure

Étape 1 Cliquez sur **Monitoring** (Superviser) dans le menu principal pour ouvrir la page Dashboards (Tableaux de bord).

Vous pouvez sélectionner des plages de temps prédéfinies, comme la dernière heure ou la dernière semaine, ou définir une plage de temps personnalisée avec des heures de début et de fin spécifiques, pour contrôler les données affichées dans les graphiques et les tableaux du tableau de bord.

Les tableaux de bord liés au trafic comprennent les types d'affichage suivants :

- Top 5 bar graphs (5 principaux graphiques à barres) : ils sont affichés dans le tableau de bord **Network Overview** (Aperçu du réseau) et dans les tableaux de bord récapitulatifs par élément que vous voyez si vous cliquez sur un élément dans un tableau de bord. Vous pouvez faire basculer les informations entre le nombre de **Transactions** ou **Data Usage** (l'utilisation des données) (total des octets envoyés et reçus). Vous pouvez également faire basculer l'affichage pour afficher toutes les transactions, les transactions autorisées ou les transactions refusées. Cliquez sur le lien **View More** (Afficher plus) pour voir le tableau associé au graphique.
- Tables (Tableaux) : les tableaux affichent les éléments d'un type particulier (par exemple, applications ou URL categories (catégories d'URL Web)) avec le nombre total de transactions de cet élément, les transactions autorisées, les transactions bloquées, l'utilisation des données et les octets envoyés et reçus. Vous pouvez faire basculer les nombres entre **les valeurs** brutes et **les pourcentages**, et afficher les 10, 100 ou 1 000 principales entrées. Si l'élément est un lien, cliquez dessus pour afficher un tableau de bord récapitulatif avec des informations plus détaillées.

Étape 2 Cliquez sur les liens **Dashboard** (Tableau de bord) dans la table des matières pour afficher les tableaux de bord pour les données suivantes :

- **Network Overview**(Aperçu du réseau) : affiche des renseignements récapitulatifs sur le trafic dans le réseau, y compris les règles d'accès (politiques) correspondantes, les utilisateurs lançant le trafic, les applications utilisées dans les connexions, les menaces de prévention des intrusions (signatures) correspondantes, les web categories (catégories d'URL Web)) pour les URL consultées et les destinations les plus fréquentes pour les connexions.
- **Users (Utilisateurs)** : affiche les principaux utilisateurs de votre réseau. Vous devez configurer les politiques d'identité pour voir les informations des utilisateurs. S'il n'y a pas d'identité d'utilisateur, l'adresse IP source est incluse. Vous pourriez voir les entités spéciales suivantes :

  - **Failed Authentication** (Échec de l'authentification) : l'utilisateur a été invité à s'authentifier, mais n'a pas réussi à saisir une paire nom d'utilisateur/mot de passe valide dans le nombre maximal de tentatives autorisées. L'échec de l'authentification n'empêche pas l'utilisateur d'accéder au réseau, mais vous pouvez écrire une règle d'accès pour limiter l'accès au réseau pour ces utilisateurs.
  - **Guest** (Invité) : les utilisateurs invités sont similaires aux utilisateurs en Failed Authentication (Échec de l'authentification), sauf que votre règle d'identité est configurée pour identifier ces utilisateurs comme Guest (Invité). Les utilisateurs invités ont été invités à s'authentifier et n'ont pas réussi à le faire dans les limites du nombre maximal de tentatives.
  - **No Authentication Required** (Aucune authentification requise) : l'utilisateur n'a pas été invité à s'authentifier, car ses connexions correspondaient à des règles d'identité ne spécifiant aucune authentification.
  - **Unknown** (Inconnu) : aucun mappage d'utilisateur n'existe pour l'adresse IP et aucun échec d'authentification n'a encore été enregistré. En règle générale, cela signifie qu'aucun trafic HTTP n'a encore été vu à partir de cette adresse.

- **Applications** : affiche les principales applications, telles que HTTP, utilisées dans le réseau. Les informations sont disponibles uniquement pour les connexions qui sont inspectées. Les connexions sont inspectées si elles correspondent à une règle « autorisée » ou à une règle de blocage qui utilise des critères autres que la zone, l'adresse et le port. Ainsi, les informations d'application ne sont pas disponibles si la connexion est de confiance ou bloquée avant d'atteindre une règle nécessitant une inspection.
- **Web Applications** (Applications Web) : affiche les principales applications Web, comme Google, utilisées dans le réseau. Les conditions de collecte des informations sur les applications Web sont les mêmes que celles du tableau de bord des applications.
- **URL Categories (Catégories d'URL)** : affiche les principales catégories de sites Web, tels que jeux d'argent ou établissements d'enseignement, qui sont utilisées dans le réseau en fonction de la catégorisation des sites Web visités. Vous devez avoir au moins une règle de contrôle d'accès qui utilise la catégorie d'URL comme critère de correspondance de trafic pour obtenir ces informations. Les renseignements seront disponibles pour le trafic qui correspond à la règle ou pour le trafic qui doit être inspecté pour déterminer s'il correspond à la règle. Vous ne verrez pas les informations de catégorie (ou de réputation) pour les connexions qui correspondent à des règles antérieures à la première règle de contrôle d'accès de catégorie Web.
- **Access and SI Rules** (Règles d'accès et de Security Intelligence : affiche les principales règles d'accès et les équivalents de règles de Security Intelligence en correspondance avec le trafic réseau.
- **Zones** : affiche les principales paires de zones de sécurité pour le trafic entrant et sortant du périphérique.
- **Destinations** : affiche les principales destinations du trafic réseau.
- **Attackers** (Agresseurs) : affiche les principaux attaquants, qui sont la source des connexions qui déclenchent les incidents d'intrusion. Vous devez configurer des politiques d'intrusion sur les règles d'accès pour afficher ces informations.
- **Targets** (Cibles) : affiche les cibles principales des incidents d'intrusion, qui sont les victimes d'une attaque. Vous devez configurer des politiques d'intrusion sur les règles d'accès pour afficher ces informations.
- **Threats** (Menaces) : affiche les principales règles d'intrusion qui ont été déclenchées. Vous devez configurer des politiques d'intrusion sur les règles d'accès pour afficher ces informations.

- **File Logs** (Journaux de fichiers) : affiche les principaux types de fichiers vus dans le trafic réseau. Vous devez configurer des politiques de fichiers sur les règles d'accès pour afficher ces informations.
- **Malware** (Programmes malveillants) : affiche les principales combinaisons d'actions et de dispositions des programmes malveillants. Vous pouvez faire un zoom avant pour afficher les renseignements sur les types de fichiers associés. Vous devez configurer des politiques de fichiers sur les règles d'accès pour afficher ces informations.
  - Les actions possibles sont : Malware Cloud Lookup (Recherche dans le nuage de programmes malveillants), Block (Blocage), Archive Block (Encrypted) (Blocage d'archive – chiffré), Detect (Détection), Custom Detection (Détection personnalisée), Cloud Lookup Timeout (Expiration de la requête de recherche dans le nuage), Malware Block (Blocage de programmes malveillants), Archive Block (Depth Exceeded) (Blocage d'archive – profondeur dépassée), Custom Detection Block (Blocage de détection personnalisée), TID Block (Blocage TID), Archive Block (Failed to Inspect) (Blocage d'archive – échec de l'inspection).
  - Les dispositions possibles sont : Malware (Programme malveillant), Unknown (Inconnu), Clean (Propre), Custom Detection (Détection personnalisée), Unavailable (Non disponible).
- **SSL Decryption** (Déchiffrement SSL) : affiche la répartition du trafic chiffré et en texte brut via le périphérique, ainsi que la répartition de la façon dont le trafic chiffré a été déchiffré selon les règles de déchiffrement SSL.
- **System (Système)** : affiche une vue globale du système, y compris un affichage des interfaces et de leur état (passez le curseur sur une interface pour voir ses adresses IP), le débit moyen global du système (en tranches de 5 minutes jusqu'à une heure, puis en tranches d'une heure pour des périodes plus longues), ainsi que des renseignements récapitulatifs sur les événements du système, l'utilisation du processeur, l'utilisation de la mémoire et l'utilisation du disque. Vous pouvez restreindre le graphique de débit pour afficher une interface précise plutôt que toutes les interfaces.

  Remarque
  Les informations affichées dans le tableau de bord System (Système) se trouvent au niveau général du système. Si vous vous connectez à l'interface de ligne de commande du périphérique, vous pouvez utiliser diverses commandes pour afficher des informations plus détaillées. Par exemple, les commandes **show cpu** et **show memory** comprennent des paramètres pour afficher d'autres détails, alors que ces tableaux de bord affichent les données des commandes **show cpu system** et **show memory system**.

Étape 3 Vous pouvez également cliquer sur ces liens dans la table des matières :

- **Events (Événements)** : pour afficher les événements à mesure qu'ils se produisent. Vous devez activer la journalisation des connexions dans les règles d'accès individuelles pour voir les événements de connexion liés à ces règles. Activez également la journalisation dans la politique Security Intelligence et les règles de déchiffrement SSL pour voir les événements Security Intelligence et obtenir des données d'événements de connexion supplémentaires. Ces événements peuvent vous aider à résoudre les problèmes de connexion de vos utilisateurs.
- **Sessions** : pour afficher et gérer les sessions utilisateur Gestionnaire de périphériques de pare-feu. Pour en savoir plus, consultez Gérer les sessions des utilisateurs Gestionnaire de périphériques de pare-feu, à la page 847.

Surveillance de statistiques supplémentaires à l'aide de l'interface de ligne de commande

Les tableaux de bord Gestionnaire de périphériques de pare-feu fournissent une grande variété de statistiques liées au trafic passant par le périphérique et à l'utilisation générale du système. Cependant, vous pouvez obtenir des informations supplémentaires sur les domaines non couverts par les tableaux de bord en utilisant la console d'interface de ligne de commande ou en vous connectant à l'interface de ligne de commande du périphérique (voir Connexion avec l'interface de ligne de commande (CLI), à la page 18).

L'interface de ligne de commande comprend une variété de commandes **show** pour fournir ces statistiques. Vous pouvez également utiliser l'interface de ligne de commande pour le dépannage général, y compris des commandes telles que **ping** et **traceroute**. La plupart des commandes **show** ont des commandes associées **clear** pour réinitialiser les statistiques à 0. (Vous ne pouvez pas effacer les statistiques à partir de la console d'interface de ligne de commande.)

Vous pouvez trouver la documentation pour les commandes dans Référence de commande Cisco Firepower Threat Defense, http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.

Par exemple, vous pourriez trouver les commandes suivantes généralement utiles.

- **show nat** affiche le nombre d'occurrences pour vos règles de NAT.
- **show xlate** affiche les traductions NAT actuellement actives.
- **show conn** fournit des renseignements sur les connexions actuelles passant par le périphérique.
- **show dhcpd** fournit des renseignements sur les serveurs DHCP que vous configurez sur les interfaces.
- **show interface** fournit des statistiques d'utilisation pour chaque interface.

Affichage des événements

Vous pouvez afficher les événements générés par vos politiques de sécurité qui permettent la journalisation. Des événements sont également générés pour les politiques de prévention des intrusions et de fichiers qui sont déclenchées.

Le tableau du visualiseur d'événements affiche les événements générés en temps réel. À mesure que de nouveaux événements sont générés, les événements plus anciens sont sortis de la table.

Avant de commencer

La génération d'événements de types particuliers dépend des éléments suivants en plus des connexions qui correspondent à la politique associée :

- Événements de connexion : une règle d'accès doit activer la journalisation des connexions. Vous pouvez aussi activer la journalisation des connexions dans la politique de renseignements sur la sécurité et dans les règles de déchiffrement SSL.
- Événements d'intrusion : une règle d'accès doit appliquer une politique de prévention des intrusions.

- Événements liés aux fichiers et aux programmes malveillants : une règle d'accès doit appliquer une politique de fichiers et activer la journalisation des fichiers.
- Événements liés aux renseignements sur la sécurité : vous devez activer et configurer la politique de renseignements sur la sécurité et activer la journalisation.

Procédure

Étape 1 Cliquez sur **Monitoring** (Surveillance) dans le menu principal.

Étape 2 Sélectionnez **Events** (Événements) dans la table des matières.

La visionneuse d'événements organise les événements sur des onglets en fonction des types d'événement. Pour en savoir plus, consultez Types d'événements, à la page 105.

Étape 3 Cliquez sur l'onglet qui affiche le type d'événement que vous souhaitez afficher.

Vous pouvez effectuer les opérations suivantes avec la liste d'événements :

- Cliquez sur **Pause** pour arrêter l'ajout de nouveaux événements afin de pouvoir rechercher et analyser un événement plus facilement. Cliquez sur **Resume** (Reprendre) pour permettre l'affichage des nouveaux événements.
- Sélectionnez une fréquence d'actualisation différente (5, 10, 20 ou 60 secondes) pour contrôler la vitesse d'affichage des nouveaux événements.
- Créez un affichage personnalisé qui inclut les colonnes que vous souhaitez. Pour créer un affichage personnalisé, cliquez sur le bouton + dans la barre d'onglets ou cliquez sur **Add/Remove Columns** (Ajouter/Supprimer des colonnes). Vous ne pouvez pas modifier les onglets prédéfinis ; ainsi, l'ajout ou la suppression de colonnes crée un nouvel affichage. Pour en savoir plus, consultez Configuration des vues personnalisées, à la page 114.
- Pour modifier la largeur d'une colonne, cliquez sur le séparateur d'en-tête de colonne et faites-le glisser jusqu'à la largeur souhaitée.
- Passez le curseur sur un événement et cliquez sur **View Details** (Afficher les détails) pour afficher les informations complètes sur un événement. Pour obtenir une description des différents champs d'un événement, consultez Description des champs d'événement, à la page 116.

Étape 4 Si nécessaire, appliquez un filtre au tableau pour vous aider à localiser les événements souhaités en fonction de divers attributs d'événement.

Pour créer un nouveau filtre, saisissez manuellement le filtre en sélectionnant des éléments atomiques dans la liste déroulante et en entrant la valeur du filtre, ou créez un filtre en cliquant sur une cellule du tableau des événements qui contient une valeur sur laquelle vous souhaitez filtrer. Vous pouvez cliquer sur plusieurs cellules dans la même colonne pour créer une condition OU parmi les valeurs, ou cliquer sur des cellules dans différentes colonnes pour créer une condition ET parmi les colonnes. Si vous créez le filtre en cliquant sur les cellules, vous pouvez également modifier le filtre obtenu pour l'affiner. Pour plus d'informations sur la création de règles de filtrage, consultez Événements de filtrage, à la page 115.

Une fois que vous avez créé le filtre, effectuez l'une des opérations suivantes :

- Pour appliquer le filtre et mettre à jour le tableau afin d'afficher uniquement les événements qui correspondent au filtre, cliquez sur le bouton **Filter** (Filtrer).

- Pour effacer un filtre entier que vous avez appliqué et faire revenir le tableau à un état non filtré, cliquez sur **Reset Filters** (Réinitialiser les filtres) dans la zone **Filter** (Filtrer).
- Pour effacer l'un des éléments atomiques d'un filtre, passez le curseur sur l'élément et cliquez sur le **X** pour l'élément. Ensuite, cliquez sur le bouton **Filter** (Filtrer).

Configuration des vues personnalisées

Vous pouvez créer vos propres vues personnalisées afin de pouvoir voir facilement les colonnes que vous souhaitez lors de l'affichage des événements. Vous pouvez également modifier ou supprimer des vues personnalisées, bien que vous ne puissiez pas modifier ou supprimer les vues prédéfinies.

Procédure

Étape 1 Sélectionnez **Monitoring (Surveillance** > **Events (Événements)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un affichage basé sur un affichage personnalisé (ou prédéfini), cliquez sur l'onglet de l'affichage, puis cliquez sur le bouton **+** à gauche des onglets.
- Pour modifier un affichage personnalisé existant, cliquez sur l'onglet correspondant à l'affichage.

Remarque
Pour supprimer un affichage personnalisé, cliquez simplement sur le bouton **X** dans l'onglet de l'affichage. Cette suppression est irréversible.

Étape 3 Cliquez sur le lien **Add/Remove Columns** (Ajouter/Supprimer des colonnes) au-dessus du tableau des événements à droite, puis sélectionnez ou désélectionnez les colonnes jusqu'à ce que la liste sélectionnée ne comporte que les colonnes à inclure dans la vue.

Cliquez et faites glisser les colonnes entre les listes disponibles (mais non utilisées) et sélectionnées. Vous pouvez également cliquer et faire glisser les colonnes dans la liste sélectionnée pour modifier l'ordre de gauche à droite des colonnes dans le tableau. Pour une description des colonnes, consultez Description des champs d'événement, à la page 116.

Lorsque vous avez terminé, cliquez sur **OK** pour enregistrer vos modifications de colonnes.

Remarque
Si vous modifiez la sélection de colonnes lors de l'affichage d'un affichage prédéfini, un nouvel affichage est créé.

Étape 4 Si nécessaire, modifiez la largeur des colonnes en cliquant sur les séparateurs de colonne et en les faisant glisser.

Événements de filtrage

Vous pouvez créer des filtres complexes pour limiter le tableau des événements aux événements qui vous intéressent actuellement. Vous pouvez utiliser les techniques suivantes, seules ou en combinaison, pour créer un filtre :

En cliquant sur les colonnes

La façon la plus simple de créer un filtre est de cliquer sur les cellules du tableau des événements qui contiennent les valeurs sur lesquelles vous souhaitez filtrer. Cliquer sur une cellule met à jour le champ **Filter** (Filtre) avec une règle correctement formulée pour cette combinaison de valeurs et de champ. Cependant, l'utilisation de cette technique nécessite que la liste d'événements existante contienne les valeurs souhaitées.

Vous ne pouvez pas filtrer sur toutes les colonnes. Si vous pouvez filtrer sur le contenu d'une cellule, elle est soulignée lorsque vous passez le curseur dessus.

Sélection d'éléments atomiques

Vous pouvez également créer un filtre en cliquant dans le champ **Filter** (Filtre) et en sélectionnant l'élément atomique souhaité dans la liste déroulante, puis en saisissant la valeur de correspondance. Ces éléments comprennent des champs d'événement qui ne sont pas affichés sous forme de colonnes dans le tableau des événements. Ils comprennent également des opérateurs pour définir la relation entre la valeur que vous saisissez et les événements à afficher. Alors que le fait de cliquer sur les colonnes entraîne toujours un filtre « = (=) », lorsque vous sélectionnez un élément, vous pouvez également sélectionner « supérieur à (>) » ou « inférieur à (<) » pour les champs numériques.

Quelle que soit la façon dont vous ajoutez un élément au champ **Filter** (Filtre), vous pouvez effectuer une saisie dans ce champ pour ajuster l'opérateur ou la valeur. Cliquez sur **Filter** (Filtre) pour appliquer le filtre au tableau.

Opérateurs pour les filtres d'événement

Vous pouvez utiliser les opérateurs suivants dans un filtre d'événement :

=	Est égal à. L'événement correspond à la valeur spécifiée. Vous ne pouvez pas utiliser de caractères génériques.
!=	N'est pas égal à. L'événement ne correspond pas à la valeur spécifiée. Vous devez saisir le ! (point d'exclamation) pour créer une expression non égale.
>	Supérieur à. L'événement contient une valeur supérieure à la valeur spécifiée. Cet opérateur est disponible pour les valeurs numériques uniquement, telles que le port et l'adresse IP.
<	Inférieur à. L'événement contient une valeur inférieure à la valeur spécifiée. Cet opérateur est disponible pour les valeurs numériques uniquement.

Règles pour les filtres d'événements complexes

Lors de la création d'un filtre complexe qui contient plus d'un élément atomique, gardez les règles suivantes à l'esprit :

- Les éléments du même type ont une relation OU entre toutes les valeurs de ce type. Par exemple, l'inclusion de l'initiateur IP=10.100.10.10 et de l'initiateur IP=10.100.10.11 correspond aux événements qui ont l'une de ces adresses comme source de trafic.

- Les éléments de différents types ont une relation ET. Par exemple, l'inclusion de l'initiateur IP=10.100.10.10 et du port de destination/type ICMP=80 correspond aux événements qui ont cette adresse source et ce port de destination uniquement. Les événements de 10.100.10.10 vers un autre port de destination ne sont pas affichés.
- Les éléments numériques, y compris les adresses IPv4 et IPv6, peuvent préciser des plages. Par exemple, vous pourriez spécifier Destination Port=50-80 pour enregistrer tout le trafic pour les ports de cette plage. Utilisez un tiret pour séparer les numéros de début et de fin. Les plages ne sont pas autorisées pour tous les champs numériques. Par exemple, vous ne pouvez pas spécifier une plage d'adresses IP dans l'élément Source.
- Vous ne pouvez pas utiliser de caractères génériques ou d'expressions régulières.

Description des champs d'événement

Les événements peuvent contenir les informations suivantes. Vous pouvez voir ces informations lorsque vous affichez les détails de l'événement. Vous pouvez également ajouter des colonnes au tableau du Visualiseur d'événements pour afficher les informations qui vous intéressent le plus.

Voici une liste complète des champs disponibles. Tous les champs ne s'appliquent pas à tous les types d'événement. Notez que les informations disponibles pour un événement de connexion peuvent varier selon le comment, le pourquoi et le moment où le système a enregistré la connexion.

Action

Pour les événements de connexion ou de renseignements de sécurité, l'action associée à la règle de contrôle d'accès ou à l'action par défaut ayant journalisé la connexion :

Autoriser

Connexions explicitement autorisées

Confiance

Connexions de confiance. Les connexions TCP détectées par une règle de confiance dès le premier paquet ne génèrent qu'un événement de fin de connexion. Le système génère l'événement une heure après le dernier paquet de session.

Bloquer

Connexions bloquées. L'action **Block (Bloquer)** peut être associée aux critères d'accès Allow (Autoriser) dans les conditions suivantes :

- Connexions pour lesquelles un exploit a été bloqué par une politique de prévention des intrusions.
- Connexions pour lesquelles un fichier a été bloqué par une politique de fichiers.
- Connexions bloquées par les renseignements de sécurité.
- Connexions bloquées par une politique SSL.

Action par défaut

Indique que la connexion a été traitée par l'action par défaut.

Pour les événements de fichier ou de programme malveillant, l'action de règle de fichier associée à l'action de règle pour la règle à laquelle le fichier correspond et toutes les options d'action de règle de fichier associées.

Connexion autorisée

Si le système a autorisé le flux du trafic pour l'événement.

Application

L'application détectée dans la connexion.

Pertinence commerciale de l'application

La pertinence commerciale associée au trafic d'application détecté dans la connexion : très élevée, élevée, moyenne, faible ou très faible. Chaque type d'application détectée dans la connexion est pertinent sur le plan commercial; ce champ affiche la valeur la plus basse (le type de moins pertinent) de ceux-ci.

Catégories d'applications, balise d'application

Critères qui caractérisent l'application pour vous aider à comprendre la fonction de l'application.

Risque lié à l'application

Le risque associé au trafic d'application détecté lors de la connexion : très élevé, élevé, moyen, faible ou très faible. Chaque type d'application détecté lors de la connexion est associé à un risque. ce champ affiche le plus élevé d'entre eux.

Type de bloc

Le type de blocage spécifié dans la règle de contrôle d'accès correspondant au flux de trafic dans l'événement : blocage ou bloc interactif.

Application client, version du client

L'application client et la version de ce client détectées dans la connexion.

Pertinence commerciale pour le client

La pertinence commerciale associée au trafic client détecté dans la connexion : très élevée, élevée, moyenne, faible ou très faible. Chaque type de client détecté dans la connexion est associé à une pertinence commerciale ; ce champ affiche la valeur la plus basse (le type de moins pertinent) de ceux-ci.

Catégorie du client, balise du client

Critères qui caractérisent l'application pour vous aider à comprendre la fonction de l'application.

Risque lié au client

Le risque associé au trafic client détecté lors de la connexion : très élevé, élevé, moyen, faible ou très faible. Chaque type de client détecté lors de la connexion est associé à un risque ; ce champ affiche le plus élevé d'entre eux.

Connexion

L'ID unique pour le flux de trafic, généré en interne.

Indicateur de type de bloc de connexion

Le type de blocage spécifié dans la règle de contrôle d'accès correspondant au flux de trafic dans l'événement : blocage ou bloc interactif.

Octets de connexion

Le nombre total d'octets pour la connexion.

Temps de connexion

Le temps pour le début de la connexion.

Horodatage de la connexion

L'heure à laquelle la connexion a été détectée.

Connexion refusée

Si le système a refusé le flux de trafic pour l'événement.

Pays et continent de destination

Le pays et le continent de l'hôte de réception.

IP de la destination

L'adresse IP utilisée par l'hôte de réception dans un incident d'intrusion, de fichier ou de programme malveillant.

Port de destination / code ICMP ; port de destination ; Icode de destination

Le port ou le code ICMP utilisé par le répondeur de session.

Balise de groupe de sécurité de destination, nom de la balise de groupe de sécurité de destination

Le numéro et le nom de la balise de groupe de sécurité TrustSec associés à la destination, le cas échéant.

Direction

La direction de la transmission d'un fichier.

Disposition

Disposition du fichier :

Maliciels

Indique que le Cisco AMP Cloud a classé le fichier comme programme malveillant ou que l'indice de menace du fichier a dépassé le seuil de programme malveillant défini dans la politique de fichiers. L'analyse locale des programmes malveillants peut aussi marquer des fichiers comme programmes malveillants.

Sain

Indique que le Cisco AMP Cloud a classé le fichier comme propre, ou qu'un utilisateur a ajouté le fichier à la liste des fichiers propres.

Inconnu

Indique que le système a interrogé le Cisco AMP Cloud, mais qu'aucune disposition n'a été attribuée au fichier ; en d'autres termes, le Cisco AMP Cloud n'a pas classé le fichier.

Détection personnalisée

Le fichier a été ajouté à la liste des détections personnalisées.

Non disponible

Indique que le système n'a pas pu interroger le Cisco AMP Cloud. Vous pouvez voir un faible pourcentage d'événements avec cette disposition; c'est un comportement attendu.

S. O.

Indique qu'une règle de détection de fichiers ou de blocage de fichiers a traité le fichier et que le système n'a pas interrogé le Cisco AMP Cloud.

Interface de sortie, Zone de sécurité de sortie

L'interface et la zone par lesquelles la connexion est sortie du périphérique.

Routeur virtuel de sortie

Le nom du routeur virtuel, le cas échéant, auquel l'interface de destination appartient.

Événement, Type d'événement

Le type d'événement.

Secondes de l'événement, Microsecondes de l'événement

L'instant, en secondes ou en microsecondes, où l'événement a été détecté.

Catégorie de fichier

Les catégories générales de type de fichier, par exemple : documents Office, Archive, Multimédia, Fichiers exécutables, Fichiers PDF, Codé, Graphique ou fichiers système.

Horodatage de l'événement du fichier

La date et l'heure de création du fichier (ou du fichier de programme malveillant).

Nom de fichier

Nom du fichier.

Action découlant d'une règle sur un fichier

L'action associée à la règle de fichiers qui a détecté le fichier, et toutes les options d'action associées à une règle de fichier.

SHA-256 du fichier

Valeur de hachage SHA-256 du fichier.

Taille du fichier (Ko)

La taille du fichier, en kilo-octets. La taille du fichier peut être vide si le système a bloqué le fichier avant sa réception complète.

Type de fichier (File Type)

Le type de fichier, par exemple HTML ou MSEXE.

Politique sur les fichiers et les programmes malveillants

La politique de fichiers associée à la génération de l'événement.

Indicateur de type de bloc de journal de fichier

Le type de blocage indiqué dans la règle de fichiers correspondant au flux de trafic dans l'événement : block (blocage) ou interactive block (blocage interactif).

Règle de politique de pare-feu, Règle de pare-feu

La règle de contrôle d'accès ou l'action par défaut qui a géré la connexion.

Premier paquet

La date et l'heure auxquelles le premier paquet de la session a été vu.

Référent HTTP

Référent HTTP, qui représente le référent d'une URL demandée pour le trafic HTTP détecté dans la connexion (comme un site Web qui a fourni un lien vers une autre URL ou a importé un lien vers une autre URL).

Réponse HTTP

Code d'état HTTP envoyé en réponse à une requête HTTP d'un client sur une connexion.

Classification IDS

La classification à laquelle appartient la règle qui a généré l'événement.

Interface d'entrée, Zone de sécurité d'entrée

L'interface et la zone par lesquelles la connexion est entrée dans le périphérique.

Routeur virtuel d'entrée

Le nom du routeur virtuel, le cas échéant, auquel l'interface source appartient.

Octets de l'initiateur, Paquets de l'initiateur

Le nombre total d'octets ou de paquets transmis par l'initiateur de la session.

Pays et continent de l'initiateur

Le pays et le continent de l'hôte qui a lancé la session. Disponible uniquement si l'adresse IP de l'initiateur est routable.

IP de l'initiateur

L'adresse IP de l'hôte (et le nom d'hôte, si la résolution DNS est activée) qui a lancé la session dans un événement de connexion ou de renseignements de sécurité.

Résultat en ligne

Si le système a abandonné ou aurait abandonné le paquet qui a déclenché un incident d'intrusion s'il travaillait en mode en ligne. La règle déclenchée n'est pas réglée sur Drop and Generate Events (Abandonner et générer des événements).

Politique de prévention des intrusions

La politique de prévention des intrusions à laquelle la règle de prévention des intrusions, de préprocesseur ou de décodeur qui a généré l'événement a été activée.

Indicateur de type de bloc IPS

L'action de la règle de prévention des intrusions correspondant au flux de trafic dans l'événement.

Dernier paquet

La date et l'heure auxquelles le dernier paquet de la session a été vu.

Étiquette MPLS

L'étiquette de commutation multiprotocole par étiquette (MPLS) associée au paquet qui a déclenché l'incident d'intrusion.

Indicateur de type de bloc de programme malveillant

Le type de blocage indiqué dans la règle de fichiers correspondant au flux de trafic dans l'événement : block (blocage) ou interactive block (blocage interactif).

Message

Pour les événements d'intrusion, le texte explicatif de l'événement. Pour les événements de programme malveillant ou de fichier, toutes les informations supplémentaires associées à l'événement de programme malveillant.

Domaine NetBIOS

Le domaine NetBIOS utilisé dans la session

Pays et continent du client d'origine

Le pays et le continent de l'hôte client d'origine qui a lancé la session. Disponible uniquement si l'adresse IP du client d'origine est routable.

IP du client d'origine

L'adresse IP d'origine du client qui a lancé une connexion HTTP. Cette adresse est dérivée des champs d'en-tête X-Forwarded-For (XFF) ou True-Client-IP HTTP ou de leur équivalent.

Politique, Révision de la politique

La stratégie de contrôle d'accès et sa révision, qui comprend la règle d'accès (pare-feu) associée à l'événement.

Priorité

La priorité de l'événement déterminée par Cisco Talos Intelligence Group (Talos) : élevée, moyenne ou basse.

Protocole

Le protocole de transport utilisé dans la connexion.

Motif

La ou les raisons pour lesquelles la connexion a été enregistrée, dans les situations expliquées dans le tableau suivant. Ce champ est autrement vide.

Motif	Description
Blocage DNS	Le système a refusé la connexion sans inspection, en fonction du nom de domaine et des données de Security Intelligence. Une raison de blocage DNS est jumelée à une action de blocage, Domaine introuvable ou Gouffre, selon l'action de règle DNS.
Moniteur DNS	Le système aurait refusé la connexion en fonction du nom de domaine et des données Security Intelligence, mais vous avez configuré le système pour surveiller, plutôt que refuser, la connexion.
Blocage de fichiers	La connexion contient un fichier ou un programme malveillant dont le système a empêché la transmission. Un motif de blocage de fichier est toujours associé à une action de blocage de fichier.
Détection personnalisée de fichier	La connexion contient un fichier de la liste de détection personnalisée dont le système a empêché la transmission.

Motif	Description
Moniteur de fichiers	Le système a détecté un type de fichier particulier dans la connexion.
Autoriser la reprise du fichier	La transmission de fichiers a été bloquée à l'origine par une règle de blocage des fichiers ou de blocage de fichiers malveillants. Après le déploiement d'une nouvelle politique de contrôle d'accès autorisant le fichier, la session HTTP a repris automatiquement.
Blocage de reprise des fichiers	La transmission de fichiers était à l'origine autorisée par une règle de fichier Detect Files ou Malware Cloud Lookup. Après le déploiement d'une nouvelle politique de contrôle d'accès bloquant le fichier, la session HTTP s'est arrêtée automatiquement.
Blocage de prévention des intrusions	Le système a bloqué ou aurait bloqué un exploit (violation de politique de prévention des intrusions) détecté dans la connexion. Une cause de blocage de prévention des intrusions est jumelée à une action de blocage pour les exploits bloqués et d'autorisation pour les exploits qui auraient été bloqués.
Moniteur de prévention des intrusions	Le système a détecté, mais n'a pas bloqué, un exploit détecté dans la connexion. Cela se produit lorsque l'état de la règle de prévention des intrusions déclenchée est défini sur Generate Events (générer des événements).
Blocage d'adresse IP	Le système a refusé la connexion sans inspection, en fonction de l'adresse IP et des données de Security Intelligence. Un motif de blocage d'IP est toujours associé à une action de blocage.
Blocage SSL	Le système a bloqué une connexion chiffrée en fonction de la configuration d'inspection SSL. Un motif de blocage SSL est toujours associé à une action de blocage.
Blocage d'URL	Le système a refusé la connexion sans inspection, en fonction de l'URL et des données de Security Intelligence. Un motif de blocage d'URL est toujours associé à une action de blocage.

Heures de réception

La date et l'heure auxquelles l'événement a été généré.

Hôte référencé

Si le protocole de connexion est HTTP ou HTTPS, ce champ affiche le nom d'hôte utilisé par le protocole respectif.

Octets du répondeur, Paquets du répondeur

Le nombre total d'octets ou de paquets transmis par le répondeur de session.

Pays et continent du répondeur

Le pays et le continent de l'hôte qui a répondu à la session. Disponible uniquement si l'adresse IP du répondeur est routable.

IP du répondeur

L'adresse IP de l'hôte (et le nom d'hôte, si la résolution DNS est activée) du répondeur de session dans une connexion ou un événement de renseignements de sécurité.

SI Category ID (Catégorie de renseignements de sécurité)

Le nom de l'objet qui contient l'élément bloqué, tel qu'un nom d'objet de réseau ou d'URL, ou le nom d'une catégorie de flux.

Signature :

L'ID de signature pour un événement lié à un fichier ou à un programme malveillant.

Pays et continent de la source

Le pays et le continent de l'hôte d'envoi. Disponible uniquement si l'adresse IP source est routable.

IP de la source

L'adresse IP utilisée par l'hôte expéditeur dans un événement d'intrusion, de fichier ou de programme malveillant.

Port source/type ICMP ; Port source ; Type de port source

Le port ou le type ICMP utilisé par l'initiateur de la session.

Balise du groupe de sécurité source, Nom de la balise du groupe de sécurité source

Le numéro de balise du groupe de sécurité TrustSec et le nom associé à la source, le cas échéant.

Action réelle du SSL

L'action réelle que le système a appliquée à la connexion. Cette action peut différer de l'action attendue. Par exemple, une connexion peut correspondre à une règle qui applique le déchiffrement, mais qui n'a pas pu être déchiffrée pour une raison quelconque.

Action	Description
Bloquer/Bloquer avec réinitialisation	Représente les connexions chiffrées bloquées.
Déchiffrer (Resigner)	Représente une connexion sortante déchiffrée à l'aide d'un certificat de serveur re-signé.
Déchiffrer (remplacer la clé)	Représente une connexion sortante déchiffrée à l'aide d'un certificat de serveur autosigné avec une clé publique remplacée.
Déchiffrer (clé connue)	Représente une connexion entrante déchiffrée à l'aide d'une clé privée connue.
Action par défaut	Indique que la connexion a été gérée par l'action par défaut.
Ne pas déchiffrer	Représente une connexion que le système n'a pas déchiffrée.

Empreinte digitale du certificat SSL

Valeur de hachage SHA utilisée pour authentifier le certificat.

Statut du certificat SSL

Cela s'applique uniquement si vous avez configuré une condition de règle SSL État du certificat. Si le trafic chiffré correspond à une règle SSL, ce champ affiche une ou plusieurs des valeurs d'état de certificat de serveur suivantes :

- Autosigné

- Valide
- Signature non valide
- Émetteur non valide
- Expiré
- Inconnu
- Non valide pour le moment
- Retiré

Si le trafic non déchiffrable correspond à une règle SSL, ce champ affiche Not Checked (Non contrôlé).

Suite de chiffrement SSL

La suite de chiffrement utilisée dans la connexion.

Action attendue de SSL

L'action spécifiée dans la règle SSL à laquelle la connexion correspond.

Indicateurs de flux SSL

Les dix premiers indicateurs de niveau de débogage pour une connexion chiffrée.

Messages de flux SSL

Les messages SSL/TLS échangés entre le client et le serveur lors de l'établissement de liaison SSL, tels que HELLO_REQUEST et CLIENT_HELLO. Consultez http://tools.ietf.org/html/rfc5246 pour obtenir plus d'informations sur les messages échangés dans les connexions TLS.

Protocole SSL

Le nom de la politique de déchiffrement SSL appliquée à la connexion.

Règle SSL

Le nom de la règle de déchiffrement SSL appliquée à la connexion.

ID de la session SSL

L'ID de session hexadécimal négocié entre le client et le serveur lors de l'établissement de liaison.

Identifiant du billet SSL

Valeur de hachage hexadécimale des informations du ticket de session envoyées lors de l'établissement de la liaison SSL.

Catégorie d'URL SSL

La catégorie d'URL du serveur Web de destination telle qu'elle est déterminée lors du traitement du déchiffrement SSL.

Version SSL

La version SSL/TLS utilisée dans la connexion.

Indicateurs TCP

Les indicateurs TCP détectés dans la connexion.

Total des paquets

Le nombre total de paquets transmis lors de la connexion, qui comprend **lInitiator Packets** (Paquets de l'initiateur) et **Responder Packets** (Paquets du répondeur).

URL, catégorie d'URL, réputation d'URL, score de réputation d'URL

L'URL demandée par l'hôte surveillé au cours de la session ainsi que sa catégorie, sa réputation et son score de réputation associés, le cas échéant.

Pour le filtrage des demandes de recherche DNS, la catégorie et la réputation concernent le FQDN affiché dans le champ DNS Query (Requête DNS). Le champ URL sera vide, car la recherche de catégorie/réputation est effectuée pour une demande DNS plutôt que pour une demande Web.

Si le système identifie ou bloque une application SSL, l'URL demandée est dans le trafic chiffré, de sorte que le système identifie le trafic selon un certificat SSL. Pour les applications SSL, ce champ indique donc le nom usuel contenu dans le certificat.

Utilisateur

L'utilisateur associé à l'adresse IP de l'initiateur.

VLAN

L'ID de VLAN le plus à l'intérieur associé au paquet qui a déclenché l'incident.

Pertinence commerciale des applications Web

La pertinence commerciale associée au trafic d'application Web détecté dans la connexion : très élevée, élevée, moyenne, faible ou très faible. Chaque type d'application Web détectée dans la connexion a une pertinence commerciale associée ; ce champ affiche la plus faible (la moins pertinente) d'entre elles.

Catégories d'applications Web, étiquette d'application Web

Critères qui caractérisent l'application pour vous aider à comprendre la fonction de l'application.

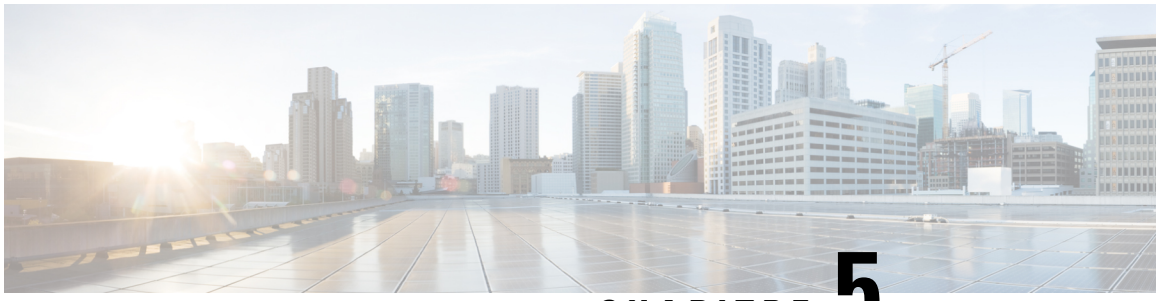
Risque lié aux applications Web

Le risque associé au trafic d'application Web détecté dans la connexion : très élevé, élevé, moyen, faible ou très faible. Chaque type d'application détecté lors de la connexion est associé à un risque; ce champ affiche le plus élevé d'entre eux.

Application Web

L'application Web, qui représente le contenu ou l'URL demandée pour le trafic HTTP détecté dans la connexion.

Si l'application Web ne correspond pas à l'URL de l'événement, le trafic est probablement référencé, comme le trafic publicitaire. Si le système détecte du trafic référencé, il stocke l'application de référence (si disponible) et répertorie cette application comme application Web.



CHAPITRE 5

Alarmes pour Cisco ISA 3000

Vous pouvez configurer le système d'alarme sur un périphérique Cisco ISA 3000 pour qu'il vous avertisse en cas de conditions indésirables.

- À propos des alarmes, à la page 127
- Valeurs par défaut pour les alarmes, à la page 129
- Configurer les alarmes pour l'ISA 3000, à la page 130
- Surveillance des alarmes, à la page 136

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 du relais d'alarme, consulter le Guide d'installation du matériel du périphérique de sécurité industrielle 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	—

Alarmes Syslog

Par défaut, le système envoie des messages syslog lorsqu'une alarme est déclenchée. Vous pouvez désactiver la messagerie syslog si vous ne souhaitez pas recevoir les messages.

Pour que les alarmes du journal système fonctionnent, vous devez également activer la journalisation des dépistages sur **Device (Périphérique)** > **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation)**. Par exemple, vous pouvez configurer un serveur syslog, la journalisation de la console ou la journalisation de la mémoire tampon interne.

Sans activation de destination pour la journalisation des dépistages, le système d'alarme n'a nulle part où envoyer les messages du journal système.

Interruptions SNMP

Vous pouvez éventuellement configurer les alarmes pour qu'elles envoient des déroutements SNMP à votre serveur SNMP. Pour que les alarmes des déroutements SNMP fonctionnent, vous devez également configurer les paramètres SNMP.

Utilisez l'API Firewall Threat Defense pour configurer SNMP. Cliquez sur le bouton des autres options () et choisissez API Explorer (Explorateur d'interface de protocole d'application). Ensuite, recherchez la ressource SNMP et examinez la documentation du modèle pour obtenir des renseignements sur la configuration de la fonctionnalité. Vous pouvez utiliser les versions SNMP 2c ou 3 ; la version 1 n'est pas prise en charge. Pour des informations complètes sur la configuration de SNMP, consultez le chapitre SNMP du *Livre 1 : Guide de configuration de l'interface de ligne de commande pour les opérations générales Cisco ASA* pour obtenir la version la plus récente du logiciel ASA. Les guides sont disponibles à l'adresse https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html.

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

	Alerte	initiales	Gravité	Interruptions SNMP	Relais de sortie	Messages de journalisation du système (syslog)
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 l'ISA 3000

Vous utilisez FlexConfig pour configurer les alarmes pour l'ISA 3000. Les rubriques suivantes expliquent comment configurer la politique.

Configurer les contacts d'entrée d'alarme

Si vous connectez les contacts d'entrée d'alarme (interfaces) à des capteurs externes, vous pouvez configurer les contacts pour qu'ils déclenchent des alarmes en fonction de l'entrée du capteur. En fait, les contacts sont activés par défaut pour envoyer des messages syslog si le contact est fermé, c'est-à-dire si le courant électrique cesser de circuler dans le contact. Vous devez configurer le contact uniquement si les valeurs par défaut ne répondent pas à vos besoins.

Les contacts d'alarme sont numérotés 1 et 2, vous devez donc comprendre comment vous avez câblé les broches physiques pour configurer les paramètres corrects. Vous configurez les contacts séparément.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Cliquez sur le bouton + pour créer un nouvel objet.

Étape 4 Saisissez un nom pour l'objet. Par exemple, **Enable_Alarm_Contact**.

Étape 5 Dans l'éditeur **Template** (Modèle), saisissez les commandes nécessaires pour configurer le contact.

a) Configurez une description pour le contact d'alarme.

alarm contact {**1** | **2**} **description** *string*

Par exemple, pour définir la description du contact 1 comme « porte ouverte », saisissez la commande suivante :

```
alarm contact 1 description Door Open
```

b) Configurez la gravité du contact d'alarme.

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

Au lieu de configurer un contact, vous pouvez utiliser **any** pour modifier la gravité de tous les contacts. La gravité contrôle le comportement du voyant DEL associé au contact.

- **major** : le voyant DEL clignote en rouge.
- **minor** : le voyant DEL est rouge en continu. Il s'agit du paramètre par défaut.
- **none** : le voyant DEL est éteint.

Par exemple, pour définir la gravité du contact 1 sur Majeur, utilisez la commande suivante :

```
alarm contact 1 severity major
```

c) Configurez le déclencheur pour le contact d'alarme.

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

Au lieu de configurer un contact, vous pouvez spécifier **any** pour modifier le déclencheur pour tous les contacts. Le déclencheur détermine la condition électrique qui déclenche une alerte.

- **open** : condition normale pour que le contact soit fermé, c'est-à-dire que le courant électrique traverse le contact. Une alerte est déclenchée si le contact s'ouvre, c'est-à-dire que le courant électrique cesser de circuler.
- **closed** : condition normale pour que le contact soit ouvert, c'est-à-dire que le courant électrique ne traverse pas le contact. Une alerte est déclenchée si le contact se ferme, c'est-à-dire que le courant électrique commence à traverser le contact. Il s'agit du paramètre par défaut.

Par exemple, vous connectez un capteur de porte au contact d'entrée d'alarme 1 et son état normal ne signifie aucun courant électrique circulant dans le contact d'alarme (il est ouvert). Si la porte est ouverte, le contact est fermé et le courant électrique traverse le contact d'alarme. Vous régleriez le déclencheur d'alarme sur fermé pour que l'alarme se déclenche lorsque le courant électrique commence à circuler.

```
alarm contact 1 trigger closed
```

d) Configurez les actions à entreprendre lorsque le contact d'alarme est déclenché.

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

Vous pouvez configurer plusieurs actions. Par exemple, vous pouvez configurer le périphérique pour activer l'alarme externe, envoyer des messages syslog et envoyer également des déroutements SNMP.

- **relais** : active le relais de sortie d'alarme, qui active l'alarme externe que vous lui avez reliée, comme une sonnerie ou un voyant clignotant. Le voyant DEL de sortie devient également rouge.

- **syslog** : envoie un message syslog. Par défaut, cette option est activée.
- **notifie** : envoie un déroutement SNMP.

Par exemple, pour activer toutes les actions pour le contact d'entrée d'alarme 1, utilisez la commande suivante :

```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

Étape 6 Dans l'éditeur **Negate Template (Modèle de négation)**, saisissez les lignes nécessaires pour annuler cette configuration.

Toutes ces commandes prennent la forme **no** pour les désactiver et revenir aux paramètres par défaut. Par exemple, si votre modèle comprend tous les exemples de commandes présentés dans cette procédure, le modèle de négation serait le suivant :

```
no alarm contact 1 description Door Open
no alarm contact 1 severity major
no alarm contact 1 trigger closed
no alarm facility input-alarm 1 relay
no alarm facility input-alarm 1 syslog
no alarm facility input-alarm 1 notifies
```

Étape 7 Cliquez sur **OK** pour enregistrer l'objet.

Étape 8 Ajoutez l'objet à la politique FlexConfig.

a) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières.
b) Cliquez sur **+** dans la liste des groupes.
c) Sélectionnez l'objet Enable_Alarm_Contact et cliquez sur **OK**.

L'aperçu doit être mis à jour avec les commandes du modèle. Vérifiez que vous voyez les commandes attendues.

d) Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant déployer la politique.

Étape 9 Une fois le déploiement terminé, dans la console d'interface de ligne de commande ou une session SSH, utilisez la commande **show running-config** et vérifiez que la configuration en cours d'exécution comporte les modifications correctes. Testez le capteur externe pour vérifier que les alarmes sont déclenchées.

Configurer les alarmes d'alimentation

L'ISA 3000 comporte deux blocs d'alimentation. Par défaut, le système fonctionne en mode d'alimentation unique. Cependant, vous pouvez configurer le système pour qu'il fonctionne en mode double, dans lequel le deuxième bloc d'alimentation fournit automatiquement l'alimentation si le bloc principal tombe en panne. Lorsque vous activez le mode double, l'alarme du bloc d'alimentation est automatiquement activée pour envoyer des alertes du journal système, mais vous pouvez désactiver complètement l'alerte ou activer les déroutements SNMP ou le relais matériel d'alarme.

La procédure suivante explique comment activer le mode double et comment configurer les alarmes du bloc d'alimentation.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Cliquez sur le bouton **+** pour créer un nouvel objet.

Étape 4 Saisissez un nom pour l'objet. Par exemple, **Enable_Power_Supply_Alarm**.

Étape 5 Dans l'éditeur **Template** (Modèle), saisissez les commandes nécessaires pour configurer l'alarme du bloc d'alimentation.

a) Activez le mode d'alimentation double.

power-supply dual

Par exemple :

```
power-supply dual
```

b) Configurez les actions à entreprendre lorsque l'alarme d'alimentation est déclenchée.

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

Vous pouvez configurer plusieurs actions. Par exemple, vous pouvez configurer le périphérique pour activer l'alarme externe, envoyer des messages syslog et envoyer également des déroutements SNMP.

- **relais** : active le relais de sortie d'alarme, qui active l'alarme externe que vous lui avez reliée, comme une sonnerie ou un voyant clignotant. Le voyant DEL de sortie devient également rouge.
- **syslog** : envoie un message syslog. Par défaut, cette option est activée.
- **notifie** : envoie un déroutement SNMP.
- **désactiver** : pour désactiver l'alarme du bloc d'alimentation. Toutes les autres actions configurées pour l'alarme de bloc d'alimentation ne sont pas opérationnelles.

Par exemple, pour activer toutes les actions pour l'alarme du bloc d'alimentation, utilisez la commande suivante :

```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

Étape 6 Dans l'éditeur **Negate Template (Modèle de négation)**, saisissez les lignes nécessaires pour annuler cette configuration.

Toutes ces commandes prennent la forme **no** pour les désactiver et revenir aux paramètres par défaut. Par exemple, si votre modèle comprend tous les exemples de commandes présentés dans cette procédure, le modèle de négation serait le suivant :

```
no power-supply dual
no alarm facility power-supply rps relay
no alarm facility power-supply rps syslog
no alarm facility power-supply rps notifies
```

Étape 7 Cliquez sur **OK** pour enregistrer l'objet.

Étape 8 Ajoutez l'objet à la politique FlexConfig.

a) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières.
b) Cliquez sur **+** dans la liste des groupes.
c) Sélectionnez l'objet Enable_Power_Supply_Alarm et cliquez sur **OK**.

L'aperçu doit être mis à jour avec les commandes du modèle. Vérifiez que vous voyez les commandes attendues.

d) Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant déployer la politique.

Étape 9 Une fois le déploiement terminé, dans la console d'interface de ligne de commande ou une session SSH, utilisez la commande **show running-config** et vérifiez que la configuration en cours d'exécution comporte les modifications correctes.

Configurer les alarmes de température

Vous pouvez configurer des alarmes en fonction de la température de la carte CPU dans le périphérique.

Vous pouvez définir une plage de températures principale et secondaire. Si la température descend sous le seuil bas ou dépasse le seuil haut, l'alarme est déclenchée.

L'alarme de température principale est activée par défaut pour toutes les actions d'alarme : relais de sortie, syslog et SNMP. Les paramètres par défaut pour la plage de température principale sont de -40 °C à 92 °C.

L'alarme de température secondaire est désactivée par défaut. Vous pouvez définir la température secondaire dans une plage de -35 °C à 85 °C.

Comme la plage de températures secondaire est plus restrictive que la plage principale, si vous définissez la température secondaire, ce paramètre désactive le paramètre principal correspondant, même si vous configurez des valeurs autres que celles par défaut pour le paramètre principal. Vous ne pouvez pas activer deux alarmes de température élevée et deux alarmes de température basse distinctes.

Ainsi, en pratique, vous devez configurer le paramètre principal uniquement ou secondaire uniquement sur élevée ou faible.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Cliquez sur le bouton **+** pour créer un nouvel objet.

Étape 4 Saisissez un nom pour l'objet. Par exemple, **Enable_Temperature_Alarm**.

Étape 5 Dans le **Template editor** (Éditeur de modèles), saisissez les commandes nécessaires pour configurer l'alarme de température.

a) Configurez la plage de températures acceptables.

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

La température est en degrés centigrades. La plage autorisée pour l'alarme principale est de -40 à 92, qui est également la plage par défaut. La plage autorisée pour l'alarme secondaire est de -35 à 85. La valeur faible doit être inférieure à la valeur élevée.

Par exemple, pour définir une plage de température plus restrictive de -20 à 80, qui se trouve dans la plage autorisée pour l'alarme secondaire, configurez l'alarme secondaire comme suit :

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

b) Configurez les actions à entreprendre lorsque l'alarme de température se déclenche.

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

Vous pouvez configurer plusieurs actions. Par exemple, vous pouvez configurer le périphérique pour activer l'alarme externe, envoyer des messages syslog et envoyer également des déroutements SNMP.

- **relais** : active le relais de sortie d'alarme, qui active l'alarme externe que vous lui avez reliée, comme une sonnerie ou un voyant clignotant. Le voyant DEL de sortie devient également rouge.
- **syslog** : envoie un message syslog.
- **notifie** : envoie un déroutement SNMP.

Par exemple, pour activer toutes les actions pour l'alarme de température secondaire, utilisez la commande suivante :

```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

Étape 6 Dans l'éditeur **Negate Template** (Modèle d'annulation), saisissez les lignes nécessaires pour annuler cette configuration.

Toutes ces commandes prennent la forme d'une **no** permettant soit de revenir aux paramètres par défaut (pour l'alarme principale), soit de les désactiver (pour l'alarme secondaire). Par exemple, si votre modèle comprend tous les exemples de commandes présentés dans cette procédure, le modèle de négation serait le suivant :

```
no alarm facility temperature secondary low -20
no alarm facility temperature secondary high 80
no alarm facility temperature secondary relay
no alarm facility temperature secondary syslog
no alarm facility temperature secondary notifies
```

Étape 7 Cliquez sur **OK** pour enregistrer l'objet.

Étape 8 Ajoutez l'objet à la politique FlexConfig.

a) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières.
b) Cliquez sur **+** dans la liste des groupes.
c) Sélectionnez l'objet Enable_Temperature_Alarm et cliquez sur **OK**.

L'aperçu doit être mis à jour avec les commandes du modèle. Vérifiez que vous voyez les commandes attendues.

d) Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant déployer la politique.

Étape 9 Une fois le déploiement terminé, dans la console d'interface de ligne de commande ou une session SSH, utilisez la commande **show running-config** et vérifiez que la configuration en cours d'exécution comporte les modifications correctes.

Surveillance des alarmes

Les rubriques suivantes expliquent comment surveiller et gérer les alarmes.

Surveillance de l'état d'alarme

Vous pouvez utiliser les commandes suivantes dans l'interface de ligne de commande pour surveiller les alarmes.

- **show alarm settings**

  Affiche la configuration actuelle pour chaque alarme possible.

- **show environment alarm-contact**

  Affiche des informations sur l'état physique des contacts d'alarme d'entrée.

- **show facility-alarm relay**

  Affiche des renseignements sur les alarmes qui ont déclenché le relais de sortie.

- **show facility-alarm status** [**info** | **major** | **minor**]

  Affiche des renseignements sur toutes les alarmes qui ont été déclenchées. Vous pouvez limiter l'affichage en utilisant le filtrage **major** ou l'état **minor**. Le mot-clé **info** produit le même résultat que l'utilisation d'aucun mot-clé.

Surveillance des messages Syslog pour des alarmes

Selon le type d'alarmes que vous configurez, les messages syslog suivants peuvent s'afficher.

Alarmes de bloc d'alimentation double

- %FTD-1-735005 : Redondance de l'unité d'alimentation OK
- %FTD-1-735006 : Perte de redondance de l'unité d'alimentation

Alarmes de température

Dans ces alarmes, la température détectée sur le périphérique est remplacée par la température détectée en degrés *Celsius*.

- %FTD-6-806001 : L'alarme principale de température de l'unité centrale de traitement est élevée en degrés *Celsius*
- %FTD-6-806002 : L'alarme principale de température élevée de l'unité centrale de traitement est supprimée

- %FTD-6-806003 : L'alarme principale de température de l'unité centrale de traitement est faible en degrés *Celsius*
- %FTD-6-806004 : L'alarme principale de température faible de l'unité centrale de traitement est effacée
- %FTD-6-806005 : L'alarme secondaire de température de l'unité centrale de traitement est élevée en degrés *Celsius*
- %FTD-6-806006 : L'alarme secondaire de température élevée de l'unité centrale de traitement est effacée
- %FTD-6-806007 : L'alarme secondaire de température de l'unité centrale de traitement est faible en degrés *Celsius*
- %FTD-6-806008 : L'alarme secondaire de température faible de l'unité centrale de traitement est effacée

Alarmes de contact d'entrée d'alarme

Dans ces alarmes, la *description* est la description du contact que vous avez configuré.

- %FTD-6-806009 : alarme activée pour AlARM_IN_1 *description_alarme_1*
- %FTD-6-806010 : alarme effacée pour AlARM_IN_1 *description_alarme_1*
- %FTD-6-806011 : alarme activée pour AlARM_IN_2 *description_alarme_2*
- %FTD-6-806012 : Alarme effacée pour AlARM_IN_2 *description_alarme_2*

Désactivation de l'alarme externe

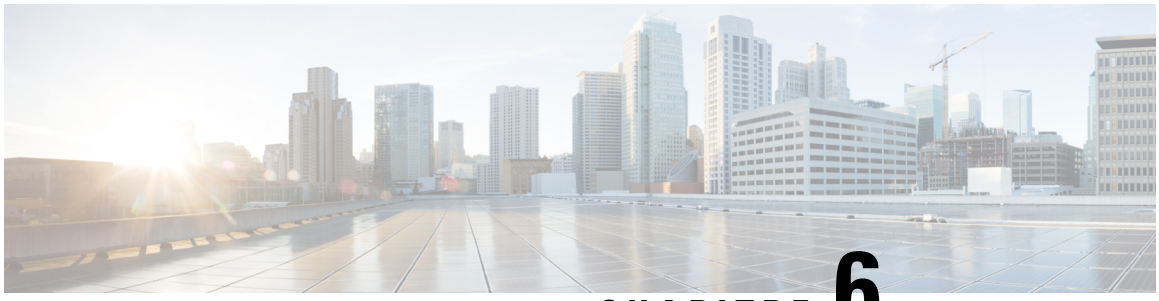
Si vous utilisez une alarme externe connectée à la sortie d'alarme et que l'alarme est déclenchée, vous pouvez désactiver cette dernière à partir de l'interface de ligne de commande du périphérique à l'aide de la commande **clear facility-alarm output**. Cette commande met la broche de sortie hors tension et éteint également le voyant DEL de sortie.



PARTIE II

Objets réutilisables

- Objets, à la page 141
- Certificats, à la page 157
- Sources d'identité, à la page 167



CHAPITRE 6

Objets

Les objets sont des conteneurs réutilisables qui définissent les critères que vous souhaitez utiliser dans les politiques ou d'autres paramètres. Par exemple, les objets réseau définissent les adresses d'hôte et de sous-réseau.

Les objets vous permettent de définir des critères afin de pouvoir réutiliser facilement les mêmes critères dans différentes politiques. Lorsque vous mettez à jour un objet, toutes les politiques qui utilisent l'objet sont automatiquement mises à jour.

- Types d'objets, à la page 141
- Lignes directrices et limites relatives aux objets, à la page 144
- Gestion des objets, à la page 145

Types d'objets

Vous pouvez créer les types d'objets suivants. Dans la plupart des cas, si une politique ou un paramètre autorise un objet, vous devez utiliser un objet.

Type d'objet	Utilisation principale	Description
Profil client AnyConnect	VPN d'accès à distance.	Les profilsclient AnyConnect sont téléchargés sur les clients avec le logiciel client AnyConnect. Ces profils définissent de nombreuses options liées au client, telles que la connexion automatique au démarrage et la reconnexion automatique, et si l'utilisateur final peut modifier l'option à partir des client AnyConnect préférences et des paramètres avancés. Consultez Configurer et charger les profils client AnyConnect, à la page 713.
Filtre d'application	Règles de contrôle d'accès.	Un objet de filtre d'application définit les applications utilisées dans une connexion IP ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. Vous pouvez utiliser ces objets dans les politiques pour contrôler le trafic au lieu d'utiliser les spécifications de port. Consultez Configuration des objets de filtre d'application, à la page 149.

Type d'objet	Utilisation principale	Description
Certificats	Politiques d'identité VPN d'accès à distance Règles de déchiffrement SSL. Serveur Web de gestion.	Les certificats numériques fournissent une identification numérique aux fins d'authentification. Les certificats sont utilisés pour les connexions SSL (Secure socket Layer), TLS (Transport Layer Security) et DTLS (Datagram TLS), comme HTTPS et LDAPS. Consultez Configurer les certificats, à la page 160.
Groupes DNS	Paramètres DNS pour les interfaces de gestion et de données.	Les groupes DNS définissent une liste de serveurs DNS et de certains attributs associés. Les serveurs du système de noms de domaine (DNS) résolvent les noms de domaine complets (FQDN), tels que www.exemple.com, en adresses IP. Consultez Configuration des groupes DNS, à la page 797.
Event List Filters (Filtres de liste d'événements)	Paramètres de journalisation système pour sélectionner les destinations de journalisation.	(Filtres du journal d'événements) et Event List Filters (Filtres de liste d'événements) créent une liste de filtres personnalisée pour les messages syslog. Vous pouvez les utiliser pour limiter les messages envoyés à un emplacement de journalisation particulier, tel qu'un serveur syslog ou le tampon de journal interne. Consultez Configurer Event List Filters (Filtres de liste d'événements), à la page 793.
Géolocalisation	Politiques de sécurité.	Un objet de géolocalisation définit les pays et les continents qui hébergent le périphérique qui est la source ou la destination du trafic. Vous pouvez utiliser ces objets dans les politiques pour contrôler le trafic au lieu d'utiliser des adresses IP. Consultez Configuration des objets de géolocalisation, à la page 153.
Sources d'identité	Politiques d'identité VPN d'accès à distance Accès Gestionnaire de périphériques de pare-feu	Les sources d'identité sont des serveurs et des bases de données qui définissent les comptes utilisateur. Vous pouvez utiliser ces informations de diverses manières, par exemple pour fournir l'identité de l'utilisateur associée à une adresse IP ou authentifier des connexions VPN d'accès à distance ou l'accès à Gestionnaire de périphériques de pare-feu. Consultez Sources d'identité, à la page 167.
Politique IKE	VPN	Les objets de politique Internet Key Exchange (IKE) définissent la proposition IKE utilisée pour authentifier les homologues IPsec, négocier et distribuer les clés de chiffrement IPsec, et établir automatiquement des associations de sécurité IPsec (SA). Il existe des objets distincts pour IKEv1 et IKEv2. Consultez Configuration de la politique IKE globale, à la page 674.

Type d'objet	Utilisation principale	Description
Proposition IPsec	VPN	Les objets Proposition IPsec configurent la proposition IPsec utilisée lors des négociations de la phase 2 d'IKE. La proposition IPsec définit la combinaison de protocoles et d'algorithmes de sécurité qui sécurisent le trafic dans un tunnel IPsec. Il existe des objets distincts pour IKEv1 et IKEv2. Consultez Configuration des propositions IPsec, à la page 679.
Réseau	Politiques de sécurité et une vaste gamme de paramètres de périphérique.	Les groupes de réseaux et les objets réseau (collectivement appelés objets réseau) définissent les adresses des hôtes ou des réseaux. Consultez Configuration des objets et des groupes de réseau., à la page 145.
Port	Politiques de sécurité.	Les groupes de ports et les objets de port (collectivement appelés objets de port) définissent les protocoles, les ports ou les services ICMP pour le trafic. Consultez Configuration des objets et groupes de ports, à la page 147.
Clés secrètes	Politiques Smart CLI et FlexConfig.	Les objets de clé secrète définissent des mots de passe ou d'autres chaînes d'authentification que vous souhaitez chiffrer et masquer. Consultez Configuration des objets de clé secrète, à la page 892.
Zone de sécurité	Politiques de sécurité.	Une zone de sécurité est un regroupement d'interfaces. Les zones divisent le réseau en segments pour vous aider à gérer et à classer le trafic. Consultez Configuration des zones de sécurité, à la page 148.
Groupes SGT	Politiques de contrôle d'accès.	Les balises de groupe de sécurité TrustSec (SGT) définissent des balises pour le trafic, conformément à la définition utilisée dans Cisco Identity Services Engine (ISE). Vous devez configurer ISE avant de pouvoir créer ces objets. Vous pouvez ensuite utiliser les objets comme critères de correspondance source/destination dans les règles de contrôle d'accès. Consultez Configuration des groupes de balises de groupe de sécurité (SGT), à la page 156.
Moniteurs SLA	Routes statiques	Un moniteur SLA définit une adresse IP cible à utiliser pour surveiller une route statique. Si le moniteur détermine que l'adresse IP cible ne peut plus être atteinte, le système peut installer une route statique de sauvegarde. Consultez Configurer les objets du moniteur SLA, à la page 326.

Type d'objet	Utilisation principale	Description
Chiffrements SSL	Paramètres SSL	Un objet de chiffrement SSL définit une combinaison de niveau de sécurité, de versions de protocole TLS/DTLS et d'algorithmes de chiffrement qui peuvent être utilisés lors de l'établissement d'une connexion SSL avec Firewall Threat Defense. Utilisez ces objets dans les paramètres système pour définir les exigences de sécurité pour les utilisateurs qui établissent des connexions TLS/SSL avec le boîtier. Consultez Configuration des paramètres de chiffrement TLS/SSL, à la page 815.
Serveurs journal système	Règles de contrôle d'accès Journalisation diagnostique. Politiques de renseignements sur la sécurité Règles de déchiffrement SSL. Politiques de prévention des intrusions Politique sur les fichiers et les programmes malveillants	Un objet serveur Syslog identifie un serveur qui peut recevoir des messages en mode connexion ou des messages de dépistage du journal système (syslog). Consultez Configuration des serveurs Syslog, à la page 154.
URL	Règles de contrôle d'accès Politiques de renseignements sur la sécurité	Les objets et groupes d'URL définissent les adresses URL ou IP des requêtes Web. Consultez Configuration des objets et groupes d'URL., à la page 151.
Utilisateurs	VPN d'accès à distance.	Vous pouvez créer des comptes utilisateur directement sur le périphérique pour une utilisation avec le VPN d'accès à distance. Vous pouvez utiliser les comptes d'utilisateurs locaux au lieu ou en plus d'une source d'authentification externe. Consultez Configurer les utilisateurs locaux, à la page 187.

Lignes directrices et limites relatives aux objets

- Les objets partagent le même espace de nom. Vous ne pouvez pas utiliser le même nom pour deux objets, même s'il s'agit de types d'objets différents.

- Le système considère les noms suivants comme réservés : Vous ne pouvez pas utiliser ces noms comme noms d'objets : objet, réseau, hôte, fqdn, no, plage, sous-réseau, description, NAT, après-auto, source, destination, statique, dynamique, any, dns, inactif, interface, service, path -pool, tourniquet, étendu, plate, inclure-reserver, tcp, udp, no-proxy-arp, recherche de routage, remarque, ID de règle, liste d'accès, ligne, ip, icmp, icmp6, avancé, ifc , groupe d'objets, vlan, journal d'événements, début de flux, fin de flux, les deux, autoriser, confiance, refuser, objet de groupe.

Gestion des objets

Vous pouvez configurer des objets directement à partir de la page Objects (Objets) ou les configurer lors de la modification des politiques. Les deux méthodes fournissent les mêmes résultats, un objet nouveau ou mis à jour. Utilisez donc la technique qui correspond à vos besoins du moment.

La procédure suivante explique comment créer et gérer vos objets directement à partir de la page Objects (Objets).

Remarque Lorsque vous modifiez une politique ou un paramètre, si une propriété nécessite un objet, une liste de ceux qui sont déjà définis s'affiche et vous sélectionnez l'objet approprié. Si l'objet souhaité n'existe pas encore, cliquez simplement sur le lien **Create New Object** (Créer un nouvel objet) affiché dans la liste.

Procédure

Étape 1 Sélectionnez **Objects** (Objets).

La page des objets comporte une table des matières répertoriant les types d'objets disponibles. Lorsque vous sélectionnez un type d'objet, vous voyez une liste des objets existants et vous pouvez en créer de nouveaux à partir d'ici. Vous pouvez également voir le contenu et le type de l'objet.

Étape 2 Sélectionnez le type d'objet dans la table des matières et effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +. Le contenu des objets diffère en fonction du type; consultez la rubrique de configuration pour chaque type d'objet pour obtenir des renseignements précis.
- Pour créer un objet de groupe, cliquez sur le bouton **Add Group** (Ajouter un groupe) ( ). Les objets de groupe comprennent plusieurs éléments.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet. Vous ne pouvez pas modifier le contenu d'un objet prédéfini.
- Pour supprimer un objet, cliquez sur l'icône de suppression ( ) de l'objet. Vous ne pouvez pas supprimer un objet s'il est utilisé dans une politique ou dans un autre objet, ou s'il s'agit d'un objet prédéfini.

Configuration des objets et des groupes de réseau.

Utilisez les groupes d'objets réseau et les objets réseau (désignés collectivement comme des objets réseau) pour définir les adresses des hôtes ou des réseaux. Vous pouvez ensuite utiliser les objets dans les politiques

de sécurité pour définir les critères de correspondance du trafic, ou dans les paramètres pour définir les adresses des serveurs ou d'autres ressources.

Un objet réseau définit un seul hôte ou une adresse réseau, alors qu'un objet de groupe de réseau peut définir plusieurs adresses.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets réseau lors de la modification d'une propriété d'adresse en cliquant sur le lien **Create New Network** (Créer un nouveau réseau) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **Network** (Réseau) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour créer un groupe, cliquez sur le bouton **Add Group** (ajouter un groupe) ( ).
- Pour modifier un objet ou un groupe, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Saisissez un nom pour l'objet et, au besoin, une description, puis définissez le contenu de l'objet.

Nous vous recommandons de ne pas utiliser une adresse IP uniquement pour le nom afin de pouvoir déterminer facilement les noms d'objets à partir du contenu d'objets ou d'adresses IP autonomes. Si vous souhaitez utiliser une adresse IP dans le nom, préfixez-la avec quelque chose de significatif, tel que host-192.168.1.2 ou network-192.168.1.0. Si vous utilisez une adresse IP comme nom, le système ajoute une barre verticale comme préfixe, par exemple, |192.168.1.2. Gestionnaire de périphériques de pare-feu n'affiche pas de barre dans les sélecteurs d'objets, mais vous verrez cette norme de dénomination si vous examinez la configuration en cours d'utilisation à l'aide de la commande **show running-config** dans l'interface de ligne de commande.

Étape 4 Configurez le contenu de l'objet.

Objets de réseau

Sélectionnez le **Type** d'objet et configurez le contenu :

- **Network** (Réseau) : saisissez une adresse réseau dans l'un des formats suivants :
  - Réseau IPv4, masque de sous-réseau inclus, par exemple : 10.100.10.0/24 ou 10.100.10.0/255.255.255.0.
  - Réseau IPv6, préfixe inclus, par exemple : 2001:DB8:0:CD30::/60.
- **Host (**Hôte) : saisissez une adresse IP d'hôte dans l'un des formats suivants :
  - Adresse d'hôte IPv4, par exemple : 10.100.10.10.
  - Adresse d'hôte IPv6, par exemple : 2001:DB8::0DB8:800:200C:417A ou 2001:DB8:0:0:0DB8:800:200C:417A.
- **Range** (Plage) : une plage d'adresses, dont l'adresse de début et l'adresse de fin sont séparées par un trait d'union. Vous pouvez définir des plages IPv4 ou IPv6. N'incluez pas de masque ni de préfixe. Par exemple, 192.168.1.10-192.168.1.250 ou 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100.

- **FQDN** : saisissez un seul nom de domaine complet, tel que www.exemple.com. Vous ne pouvez pas utiliser de caractères génériques. Sélectionnez auss **DNS Resolution** (Résolution DNS) afin de déterminer si vous souhaitez associer au FQDN des adresses IPv4, IPv6, ou à la fois IPv4 et IPv6. La valeur par défaut est à la fois IPv4 et IPv6. Vous pouvez utiliser ces objets dans les règles de contrôle d'accès seulement. Les règles correspondent à l'adresse IP obtenue pour le FQDN par une recherche DNS.

Groupes de réseaux

Cliquez sur le bouton + pour sélectionner les objets ou les groupes réseau à ajouter au groupe. Vous pouvez également créer de nouveaux objets.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des objets et groupes de ports

Utilisez des objets de groupe et de port (collectivement appelés objets de port) pour définir les protocoles, les ports ou les services ICMP pour le trafic. Vous pouvez utiliser les objets et les groupes dans les politiques de sécurité pour définir les critères de correspondance du trafic réseau, par exemple pour utiliser des règles d'accès pour autoriser le trafic vers des ports TCP spécifiques.

Un objet de port définit un protocole unique, un port TCP/UDP ou une plage de ports ou un service ICMP, alors qu'un objet de groupe de ports peut définir plusieurs services.

Le système comprend plusieurs objets prédéfinis pour les services communs. Vous pouvez utiliser ces objets dans vos politiques. Vous ne pouvez pas modifier ou supprimer des objets définis par le système.

Remarque Lors de la création d'objets de groupe de ports, vérifiez que la combinaison des objets a du sens. Par exemple, vous ne pouvez pas avoir un mélange de protocoles dans un objet si vous l'utilisez pour spécifier les ports source et de destination dans une règle d'accès. Faites preuve de prudence lorsque vous modifiez un objet qui est déjà utilisé, sinon vous pourriez invalider (et désactiver) les politiques qui utilisent l'objet.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de port lorsque vous modifiez une propriété de service en cliquant sur le lien **Create New Port** (Créer un nouveau port) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **Ports** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour créer un groupe, cliquez sur le bouton **Add Group** (ajouter un groupe) ( ).
- Pour modifier un objet ou un groupe, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Saisissez un nom pour l'objet et, éventuellement, une description, et définissez le contenu de l'objet.

Objets de port

Sélectionnez le **protocole**, puis configurez-le comme suit :

- **TCP**, **UDP** : saisissez le numéro de port unique ou de plage de ports, par exemple, 80 (pour HTTP) ou 1-65535 (pour couvrir tous les ports).
- **ICMP**, **IPv6-ICMP** : sélectionnez le **type ICMP** et éventuellement, le **code**. Sélectionnez **Any** (Tous) pour le type à appliquer à tous les messages ICMP. Pour en apprendre davantage sur les types et les codes, consultez les pages suivantes :
  - ICMP—http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6—http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- **Other** (Autre) : sélectionnez le protocole souhaité.

Groupes de ports

Cliquez sur le bouton **+** pour sélectionner les objets de port à ajouter au groupe. Vous pouvez également créer de nouveaux objets.

Étape 4 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des zones de sécurité

Une zone de sécurité est un regroupement d'interfaces. Les zones divisent le réseau en segments pour vous aider à gérer et à classer le trafic. Vous pouvez définir plusieurs zones, mais une interface donnée ne peut se trouver que dans une seule zone.

Le système crée les zones suivantes lors de la configuration initiale. Vous pouvez modifier ces zones pour ajouter ou supprimer des interfaces, ou vous pouvez supprimer les zones si vous ne les utilisez plus.

- **inside_zone** : Comprend l'interface interne. Si l'interface interne est un groupe de ponts, cette zone comprend toutes les interfaces membres du groupe de ponts au lieu de l'interface virtuelle de pont (BVI) interne. Cette zone est destinée à représenter les réseaux internes.
- **outside_zone** : Comprend l'interface externe. Cette zone est destinée à représenter les réseaux en dehors de votre contrôle, comme Internet.

Généralement, vous regrouperiez les interfaces selon le rôle qu'elles jouent dans votre réseau. Par exemple, vous placeriez l'interface qui se connecte à Internet dans la zone de sécurité **outside_zone** et toutes les interfaces pour vos réseaux internes dans la zone de sécurité **inside_zone**. Ensuite, vous pouvez appliquer des règles de contrôle d'accès au trafic en provenance de la zone extérieure et à destination de la zone intérieure.

Avant de créer des zones, tenez compte des règles d'accès et des autres politiques que vous souhaitez appliquer à vos réseaux. Par exemple, vous n'avez pas besoin de mettre toutes les interfaces internes dans la même zone. Si vous avez quatre réseaux internes et que vous souhaitez en traiter un différemment des trois autres, vous pouvez créer deux zones plutôt qu'une. Si vous avez une interface qui devrait permettre un accès externe à un serveur Web public, vous pouvez utiliser une zone distincte pour l'interface.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des zones de sécurité lorsque vous modifiez une propriété de zone

de sécurité en cliquant sur le lien **Create New Security Zone** (créer une nouvelle zone de sécurité) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (objets), puis **Security Zones** (zones de sécurité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Sélectionnez le **Mode** de la zone.

Cela est directement lié au mode d'interface. La zone peut contenir un seul type d'interface.

- **Routées** : les interfaces routées sont les interfaces normales pour le trafic traversant qui peuvent appliquer des politiques de sécurité.
- **Passives** : les interfaces passives n'affectent pas le trafic qui traverse le périphérique.

Étape 5 Dans la liste des **Interfaces**, cliquez sur **+** et sélectionnez les interfaces à ajouter à la zone.

La liste affiche toutes les interfaces nommées qui ne sont pas actuellement dans une zone. Vous devez configurer une interface et lui donner un nom avant de pouvoir l'ajouter à une zone.

Si toutes les interfaces nommées sont déjà dans des zones, la liste est vide. Si vous essayez de déplacer une interface vers une autre zone, vous devez d'abord la retirer de sa zone actuelle.

Remarque
Vous ne pouvez pas ajouter une interface de groupe de ponts (BVI) à une zone. Au lieu de cela, ajoutez les interfaces de membres. Vous pouvez placer les membres dans différentes zones.

Étape 6 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des objets de filtre d'application

Un objet de filtre d'application définit les applications utilisées dans une connexion IP ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. Vous pouvez utiliser ces objets dans les politiques pour contrôler le trafic au lieu d'utiliser les spécifications de port.

Bien que vous puissiez préciser des applications individuelles dans la règle, les filtres d'applications simplifient la création et l'administration des politiques. Par exemple, vous pouvez créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible pertinence commerciale. Si un utilisateur tente d'utiliser l'une de ces applications, la session est bloquée.

Vous pouvez sélectionner des applications et des filtres d'application directement dans une politique sans utiliser d'objets de filtre d'application. Cependant, un objet est pratique si vous souhaitez créer plusieurs

politiques pour le même groupe d'applications ou de filtres. Le système comprend plusieurs filtres d'application prédéfinis, que vous ne pouvez ni modifier ni supprimer.

Remarque Cisco procède fréquemment à la mise à jour ou à l'ajout de détecteurs d'applications supplémentaires au moyen des mises à jour du système et de la base de données sur les vulnérabilités (VDB). Ainsi, une règle bloquant les applications à risque élevé peut s'appliquer automatiquement aux nouvelles applications sans que vous ayez à mettre à jour la règle manuellement.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de filtre d'application lors de la modification d'une règle de contrôle d'accès en cliquant sur le lien **Save As Filter** (Enregistrer en tant que filtre) après avoir ajouté des critères d'application sous l'onglet Applications.

Avant de commencer

Lors de l'édition d'un filtre, si une application sélectionnée a été supprimée par une mise à jour de VDB, « (Deprecated) » s'affiche après le nom de l'application. Vous devez supprimer ces applications du filtre, sinon les déploiements et les mises à niveau logicielles du système suivants seront bloqués.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **Application Filters** (Filtres d'applications) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Dans la liste **Applications**, cliquez sur **Add + (Ajouter +)** et sélectionnez les applications et les filtres à ajouter à l'objet.

La liste initiale affiche les applications dans une liste déroulante continuellement. Cliquez sur **Advanced Filter** (Filtre avancé) pour afficher les options de filtre et faciliter la sélection des applications. Cliquez sur **Add** (Ajouter) lorsque vous avez effectué vos sélections. Vous pouvez répéter le processus pour ajouter des applications ou des filtres supplémentaires.

Remarque
Plusieurs sélections dans un seul critère de filtre ont une relation OU. Par exemple, le risque est élevé ou très élevé. La relation entre les filtres est ET, donc le risque est élevé ou très élevé, ET la pertinence commerciale est faible ou très faible. Lorsque vous sélectionnez des filtres, la liste des applications dans l'affichage est mise à jour pour n'afficher que celles qui répondent aux critères. Vous pouvez utiliser ces filtres pour vous aider à trouver les applications que vous souhaitez ajouter individuellement ou pour vérifier que vous sélectionnez les filtres souhaités à ajouter à la règle.

Risques

La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation, de très faible à très élevée.

Pertinence commerciale

La probabilité que l'application soit utilisée dans le cadre des activités professionnelles de votre entreprise, plutôt qu'à des fins récréatives, de très faible à très élevée.

Types

Le type d'application :

- **Application Protocol** (Protocole d'application) : protocoles d'application tels que HTTP et SSH, qui représentent les communications entre les hôtes.
- **Client Protocol** (Protocole client) : clients tels que les navigateurs Web et les clients de messagerie, qui représentent les logiciels s'exécutant sur l'hôte.
- **Web Application** (Application Web) : applications Web telles que MPEG video et Facebook, qui représentent le contenu ou l'URL demandée pour le trafic HTTP.

Catégories

Une classification générale de l'application qui décrit sa fonction la plus essentielle.

Étiquettes

Des informations supplémentaires sur l'application, similaires à la catégorie.

Pour le trafic chiffré, le système peut identifier et filtrer le trafic en utilisant uniquement les applications marquées **SSL Protocol** (Protocole SSL). Les applications sans cette balise ne peuvent être détectées que dans le trafic non chiffré ou déchiffré. Le système attribue la balise de **trafic déchiffré** aux applications qu'il peut détecter dans le trafic déchiffré uniquement, non chiffré ou non déchiffré.

Liste des applications (bas de l'affichage)

Cette liste est mise à jour à mesure que vous sélectionnez des filtres dans les options au-dessus de la liste, de sorte que vous pouvez voir les applications qui correspondent actuellement au filtre. Utilisez cette liste pour vérifier que votre filtre cible les applications souhaitées lorsque vous avez l'intention d'ajouter des critères de filtre à la règle. Si votre intention est d'ajouter des applications spécifiques, sélectionnez-les dans cette liste.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des objets et groupes d'URL.

Utiliser des objets et des groupes d'URL (collectivement appelés objets d'URL) pour définir les adresses URL ou IP des requêtes Web. Vous pouvez utiliser ces objets pour mettre en œuvre le filtrage manuel d'URL dans les politiques de contrôle d'accès, ou le blocage dans les politiques Security Intelligence.

Un objet URL définit une seule URL ou adresse IP, alors qu'un objet de groupe d'URL peut définir plusieurs URL ou adresses.

Lors de la création d'objets URL, gardez les points suivants à l'esprit :

- Si vous n'incluez pas de chemin (c'est-à-dire qu'il n'y a pas de caractères / dans l'URL), la correspondance est basée sur le nom d'hôte du serveur uniquement. Si vous incluez un ou plusieurs caractères /, la chaîne URL complète est utilisée pour une correspondance de sous-chaîne. Ainsi, une URL est considérée comme en correspondance si l'une des conditions suivantes est remplie :
  - La chaîne se trouve au début de l'URL.
  - La chaîne suit un point.
  - La chaîne contient un point au début.
  - La chaîne suit les caractères ://.

  Par exemple, ign.com correspond à ign.com ou www.ign.com, mais pas à versign.com.

Remarque Nous vous recommandons de ne pas utiliser le filtrage manuel d'URL pour bloquer ou autoriser des pages Web individuelles ou des parties de sites (c'est-à-dire les chaînes URL avec des caractères /), car les serveurs peuvent être réorganisés et les pages déplacées vers de nouveaux chemins.

- Le système ne tient pas compte du protocole de chiffrement (HTTP ou HTTPS). En d'autres termes, si vous bloquez un site Web, les trafics HTTP et HTTPS vers ce site Web sont bloqués, sauf si vous utilisez une condition d'application pour cibler un protocole spécifique. Lors de la création d'un objet URL, vous n'avez pas besoin de préciser le protocole lors de la création d'un objet. Par exemple, utilisez exemple.com plutôt que http://exemple.com.
- Si vous prévoyez utiliser un objet URL pour faire correspondre le trafic HTTPS dans une règle de contrôle d'accès, créez l'objet en utilisant le nom usuel du sujet dans le certificat de clé publique utilisé pour chiffrer le trafic. De plus, le système ne tient pas compte des sous-domaines du nom usuel du sujet. N'incluez donc pas les informations de ce sous-domaine. Par exemple, utilisez exemple.com plutôt que www.exemple.com.

  Cependant, veuillez comprendre que le nom usuel du sujet dans le certificat peut être complètement sans rapport avec le nom de domaine d'un site Web. Par exemple, le nom usuel du sujet dans le certificat pour youtube.com est *.Google.com (bien entendu, cela peut changer à tout moment). Vous obtiendrez des résultats plus cohérents si vous utilisez la politique de déchiffrement SSL pour déchiffrer le trafic HTTPS afin que les règles de filtrage d'URL fonctionnent sur le trafic déchiffré.

Remarque Les objets URL ne correspondront pas au trafic HTTPS si le navigateur reprend une session TLS, car les informations de certificat ne sont plus disponibles. Ainsi, même si vous configurez soigneusement l'objet URL, vous pourriez obtenir des résultats incohérents pour les connexions HTTPS.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets URL lorsque vous modifiez une propriété d'URL en cliquant sur le lien **Create New URL** (Créer une nouvelle URL) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects (Objets)**, puis sélectionnez **URL** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour créer un groupe, cliquez sur le bouton **Add Group** (ajouter un groupe) ( ).
- Pour modifier un objet ou un groupe, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Définissez le contenu de l'objet.

Objets de l'URL

Saisissez une URL ou une adresse IP dans la boîte **URL**. Vous ne pouvez pas utiliser de caractères génériques dans l'URL.

Groupe d'URL

Cliquez sur le bouton + pour sélectionner les objets URL à ajouter au groupe. Vous pouvez également créer de nouveaux objets.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des objets de géolocalisation

Un objet de géolocalisation définit les pays et les continents qui hébergent le périphérique qui est la source ou la destination du trafic. Vous pouvez utiliser ces objets dans les politiques pour contrôler le trafic au lieu d'utiliser des adresses IP. En utilisant la localisation géographique, vous pouvez facilement restreindre l'accès à un pays en particulier sans avoir besoin de connaître toutes les adresses IP potentielles qui y sont utilisées.

Vous pouvez généralement sélectionner des emplacements géographiques directement dans une politique sans utiliser d'objets de géolocalisation. Cependant, un objet est pratique si vous souhaitez créer plusieurs politiques pour le même groupe de pays et de continents.

Remarque Pour vous assurer que vous utilisez des données de localisation géographique à jour pour filtrer votre trafic, Cisco vous recommande fortement de mettre à jour régulièrement la base de données de géolocalisation (GeoDB).

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de géolocalisation lors de la modification d'une propriété de réseau en cliquant sur le lien **Create New Geolocation** (Créer une nouvelle géolocalisation) affiché dans la liste des objets.

Procédure

Étape 1 Sélectionnez **Objects (Objets)**, puis **Geolocation** (Géolocalisation) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Dans la liste **Continents/Countries** (Continents/Pays), cliquez sur **Add** (Ajouter) et sélectionnez les continents et les pays à ajouter à l'objet.

La sélection d'un continent sélectionne tous les pays du continent.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des serveurs Syslog

Un objet serveur Syslog identifie un serveur qui peut recevoir des messages en mode connexion ou des messages de dépistage du journal système (syslog). Si vous avez un serveur syslog configuré pour la collecte et l'analyse des journaux, créez des objets pour les définir et utilisez les objets dans les politiques connexes.

Vous pouvez envoyer les types d'événements suivants au serveur syslog :

- Événements de connexion. Configurez l'objet serveur syslog sur les types de politiques suivants : règles de contrôle d'accès et action par défaut, règles de déchiffrement SSL et action par défaut, politique sur les renseignements de sécurité.
- les incidents d'intrusion. Configurez l'objet serveur syslog dans la politique de prévention des intrusions.
- Événements de diagnostic. Voir Configurer la journalisation vers un serveur Syslog distant, à la page 790.
- Événements liés aux fichiers ou aux programmes malveillants. Configurez le serveur syslog dans **Device (Appareil)** > **System Settings (Paramètres du système)** > **Logging Settings (Paramètres de journalisation)**.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de serveur syslog tout en modifiant une propriété de serveur de journal système en cliquant sur le lien **Add Syslog Server** (Ajouter un serveur syslog) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis **Syslog Servers** (Serveurs syslog) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés du serveur :

- **IP Address** (adresse IP) : saisissez l'adresse IP du serveur syslog.
- **Protocol Type** (Type de protocole), **Port Number** (Numéro de port) : sélectionnez le protocole et saisissez le numéro de port à utiliser pour syslog. La valeur par défaut est UDP/514. Si vous sélectionnez **TCP**, le système peut reconnaître lorsque le serveur syslog n'est pas disponible et arrête d'envoyer des événements jusqu'à ce que le serveur soit de nouveau disponible. Le port UDP par défaut est 514 et le port TCP par défaut est 1470. Le port doit être compris entre 1 025 et 65 535.

  Remarque
  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.

- **Interface for Device Logs** (Interface pour les journaux du périphérique) : sélectionnez l'interface à utiliser pour l'envoi de messages de dépistage syslog. Les types d'événements suivants utilisent toujours l'interface de gestion : connexion, intrusion, fichier, programme malveillant. Votre sélection d'interface détermine l'adresse IP associée aux messages syslog. Sélectionnez l'une des options suivantes :
  - **Data Interface** (interface de données) : utilisez l'interface de données que vous sélectionnez pour les messages de dépistage syslog. Si le serveur est accessible par l'intermédiaire d'une interface de membre de groupe de ponts, sélectionnez l'interface de groupe de ponts (BVI).S'il est accessible via l'interface de diagnostic (l'interface de gestion physique), nous vous recommandons de sélectionner **Management Interface** (Interface de gestion) plutôt que cette option. Vous ne pouvez pas sélectionner une interface passive.

    Pour les messages système de connexion, d'intrusion, de fichier et de programme malveillant, l'adresse IP source sera soit pour l'interface de gestion, soit pour l'interface de la passerelle si vous passez par des interfaces de données. Notez qu'il doit y avoir des routes appropriées dans la table de routage qui dirigent le trafic vers le serveur syslog via l'interface sélectionnée pour ces types d'événements.
  - **Management Interface** (Interface de gestion) : utilisez l'interface de gestion virtuelle pour tous les types de messages syslog. L'adresse IP source sera soit pour l'interface de gestion, soit pour l'interface de la passerelle si vous passez par des interfaces de données.

Étape 4 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des groupes de balises de groupe de sécurité (SGT)

Utilisez les objets de groupe de balises de sécurité (SGT) pour identifier les adresses source ou de destination en fonction d'une balise SGT attribuée par le Moteur de services d'identité (ISE). Vous pouvez ensuite utiliser les objets dans les règles de contrôle d'accès pour définir les critères de correspondance du trafic.

Vous ne pouvez pas utiliser les informations extraites d'ISE directement dans une règle de contrôle d'accès. Au lieu de cela, vous devez créer des groupes SGT, qui font référence aux informations SGT téléchargées. Vos groupes de balises SGT peuvent faire référence à plusieurs SGT, vous pouvez donc appliquer une politique basée sur les collections de balises pertinentes, le cas échéant.

Pour en savoir plus sur l'utilisation des balises SGT pour le contrôle d'accès, consultez Comment contrôler l'accès au réseau à l'aide des balises de groupe de sécurité TrustSec, à la page 532.

Avant de commencer

Avant de créer des groupes SGT, vous devez configurer la source d'identité ISE pour vous abonner aux mappages SXP et déployer les modifications. Le système récupère ensuite les informations SGT à partir du serveur ISE. Ce n'est qu'après le téléchargement des balises SGT que vous pourrez créer des groupes de SGT.

Procédure

Étape 1 Sélectionnez **Objects (Objets)**, puis sélectionnez **SGT Groups (Groupes SGT)** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un **nom** pour l'objet et, facultativement, une description,

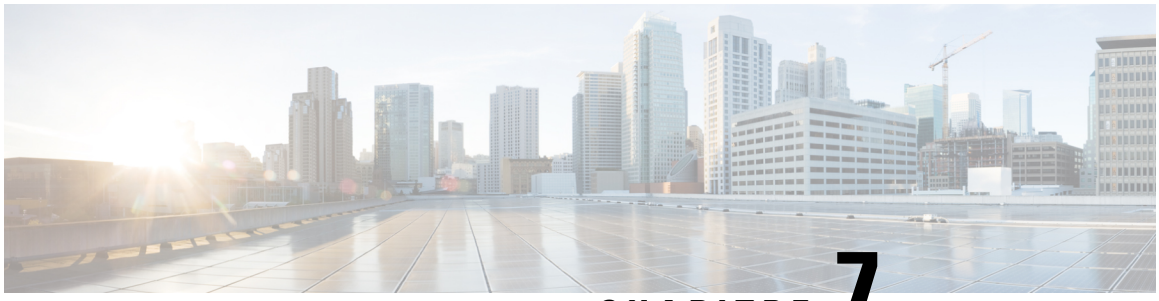
Étape 4 Sous **Tags (Balises)**, cliquez sur le signe **+** et sélectionnez les balises SGT téléchargées à inclure dans l'objet.

Pour supprimer une balise SGT, cliquez sur le **x** à droite du nom de la balise.

Si la liste est vide, le système n'a pas pu télécharger les mappages SGT. Si cela se produit :

- Assurez-vous que l'objet d'identité ISE s'abonne à la rubrique SXP. Vous devez vous abonner à SXP pour obtenir les mappages.
- Vérifiez que les mappages statiques sont définis dans ISE et qu'ISE est configuré pour publier ces mappages. S'il n'y a aucun mappage, il n'y a tout simplement rien à télécharger. Consultez Configurer les groupes de sécurité et la publication SXP dans ISE, à la page 535

Étape 5 Cliquez sur **OK**.



CHAPITRE 7

Certificats

Les certificats numériques fournissent une identification numérique aux fins d'authentification. Les certificats sont utilisés pour les connexions SSL (Secure socket Layer), TLS (Transport Layer Security) et DTLS (Datagram TLS), comme HTTPS et LDAPS. Les rubriques suivantes expliquent comment créer et gérer les certificats.

- Certificats, à la page 157
- Configurer les certificats, à la page 160

Certificats

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. Un certificat numérique comprend également une copie de la clé publique de l'utilisateur ou du périphérique. Les certificats sont utilisés pour les connexions SSL (Secure socket Layer), TLS (Transport Layer Security) et DTLS (Datagram TLS), comme HTTPS et LDAPS.

Vous pouvez créer les types de certificat suivants :

- Certificats internes : les certificats d'identité internes sont des certificats pour des systèmes ou des hôtes spécifiques. Vous pouvez les générer vous-même à l'aide de la boîte à outils OpenSSL ou les obtenir auprès d'une autorité de certification. Vous pouvez également générer un certificat autosigné. Lorsque les certificats internes expirent ou deviennent non valides pour une raison quelconque, vous pouvez les régénérer à partir de la commande CLI CLISH suivante :

```
> system support regenerate-security-keyring
  String  Certificate to be regenerated, default or fdm
```

- Certificats d'autorité de certification (CA) internes : les certificats d'autorité de certification internes sont des certificats que le système peut utiliser pour signer d'autres certificats. Ces certificats varient des certificats d'identité internes en ce qui concerne l'extension des contraintes de base et l'indicateur de l'autorité de certification, qui sont activés pour les certificats d'autorité de certification mais désactivés pour les certificats d'identité. Vous pouvez les générer vous-même à l'aide de la boîte à outils OpenSSL ou les obtenir auprès d'une autorité de certification. Vous pouvez également générer un certificat d'autorité de certification interne autosigné. Si vous configurez des certificats d'autorité de certification internes autosignés, l'autorité de certification s'exécute sur le périphérique lui-même.

- Un certificat d'une autorité de certification de confiance (CA) est utilisé pour signer d'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 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 délivrent des certificats numériques dans le cadre d'une PKI, qui utilise le chiffrement par clé publique ou privée pour assurer la sécurité. Une autorité de certification peut être un tiers de confiance, tel que VeriSign, ou une autorité de certification privée (interne) que vous établissez dans votre organisation. Les autorités de certification sont chargées de gérer les demandes de certificats et d'émettre des certificats numériques. Pour en savoir plus, consultez Chiffrement à clé publique, à la page 158.

Chiffrement à clé publique

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.

Vous pouvez en savoir plus sur les certificats numériques et le chiffrement à clé publique en vous rendant sur openssl.org, sur Wikipedia ou d'autres sources. Une bonne compréhension du chiffrement SSL/TLS vous aidera à établir des connexions sécurisées avec votre périphérique.

Types de certificats utilisés par fonctionnalité

Vous devez créer le bon type de certificat pour chaque fonctionnalité. Les fonctionnalités suivantes nécessitent des certificats.

Politiques d'identité (Identity Policies, portail captif) : certificat interne

(Facultatif) Le portail captif est utilisé dans les politiques d'identité. Les utilisateurs doivent accepter ce certificat lors de l'authentification à l'appareil afin de s'identifier et d'associer leur adresse IP à leur nom d'utilisateur. Si vous ne fournissez pas de certificat, l'appareil utilise un certificat généré automatiquement.

Identité du domaine (politiques d'identité et VPN d'accès distant) : Certificat de l'autorité de certification de confiance

(Facultatif) Si vous utilisez une connexion cryptée pour votre serveur d'annuaire, le certificat doit être accepté pour effectuer l'authentification avec le serveur d'annuaire. Les utilisateurs doivent s'authentifier lorsque les politiques VPN d'identité et d'accès à distance le demandent. Un certificat n'est pas nécessaire si vous n'utilisez pas le chiffrement pour le serveur d'annuaire.

Serveur Web de gestion (paramètres système d'accès de gestion) : Certificat interne

(Facultatif.) FDM est une demande basée sur le Web, elle fonctionne donc sur un serveur Web. Vous pouvez télécharger un certificat que votre navigateur accepte comme valide pour éviter de recevoir un avertissement d'autorité non fiable.

VPN d'accès distant : Certificat interne

(Requis) Le certificat interne est destiné à l'interface extérieure, qui établit l'identité de l'appareil pour les client AnyConnect lorsqu'ils établissent une connexion avec l'appareil. Les clients doivent accepter ce certificat.

VPN de site à site : Certificats d'autorité de certification interne et de confiance

Si vous utilisez l'authentification par certificat pour une connexion VPN de site à site, vous devez sélectionner le certificat d'identité interne utilisé pour authentifier l'homologue local dans la connexion. Bien que cela ne fasse pas partie de la définition de connexion VPN, vous devez également télécharger les certificats d'autorité de certification de confiance utilisés pour signer les certificats d'identité des homologues locaux et distants, afin que le système puisse authentifier les homologues.

SSL Decryption Policy (politique de déchiffrement SSL) : Certificats et groupes de certificats internes, d'autorité de certification interne et d'autorité de certification de confiance

(Requis) La politique de déchiffrement SSL utilise des certificats aux fins suivantes :

- Les certificats internes sont utilisés pour les règles connues de déchiffrement des clés.
- Les certificats d'autorité de certification interne sont utilisés pour déchiffrer les règles de nouvelle signature lors de la création de la session entre le client et le périphérique Firepower Threat Defense.
- Les certificats d'autorité de certification de confiance sont utilisés indirectement pour déchiffrer les règles de nouvelle signature lors de la création de la session entre le périphérique Firepower Threat Defense et le serveur. Les certificats d'autorité de certification de confiance sont utilisés pour vérifier l'autorité de signature du certificat du serveur. Vous pouvez configurer ces certificats directement ou dans un groupe de certificats dans les paramètres de politiques. Le système comprend un grand nombre de certificats d'autorité de certification de confiance, qui sont réunis dans le groupe d'autorités de confiance de Cisco. Vous n'avez donc pas besoin de télécharger de certificats supplémentaires.

Exemple : génération d'un certificat interne à l'aide d'OpenSSL

L'exemple suivant utilise les commandes OpenSSL pour générer un certificat de serveur interne. Vous pouvez obtenir OpenSSL à partir de OpenSSL.org. Consultez la documentation d'OpenSSL pour obtenir des renseignements précis. Les commandes utilisées dans cet exemple peuvent changer et vous pouvez avoir d'autres options disponibles que vous pourriez souhaiter utiliser.

Cette procédure vise à vous donner une idée de la façon d'obtenir un certificat à charger vers . Firepower Threat Defense.



Remarque Les commandes OpenSSL affichées ici ne sont que des exemples. Ajustez les paramètres en fonction de vos exigences de sécurité.

Procédure

Étape 1 Générez une clé.

```
openssl genrsa -out server.key 4096
```

Étape 2 Générez une demande de signature de certificat (CSR).

```
openssl req -new -key server.key -out server.csr
```

Étape 3 Générez un certificat autosigné avec la clé et la CSR.

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Étant donné que le Gestionnaire de périphériques de pare-feu ne prend pas en charge les clés chiffrées, essayez d'ignorer le mot de passe de défi en appuyant simplement sur Entrée lors de la génération d'un certificat autosigné.

Étape 4 Chargez les fichiers dans les champs appropriés lors de la création d'un objet de certificat interne dans Gestionnaire de périphériques de pare-feu.

Vous pouvez également copier/coller le contenu du fichier. Les exemples de commandes créent les fichiers suivants :

- server.crt : chargez ou collez le contenu dans le champ Server Certificate (Certificat de serveur).
- server.key : chargez ou collez le contenu dans le champ Certificate Key (Clé du certificat). Si vous avez fourni un mot de passe lors de la génération de la clé, vous pouvez la déchiffrer à l'aide de la commande suivante. Le résultat est envoyé à stdout, où vous pouvez le copier.

  ```
  openssl rsa -in server.key -check
  ```

Configurer les certificats

Firewall Threat Defense prend en charge les certificats X509 au format PEM ou DER. Utilisez OpenSSL pour générer des certificats si nécessaire, les obtenir d'une autorité de certification de confiance ou créer des certificats autosignés.

Pour en savoir plus sur ces certificats, consultez Certificats, à la page 157.

Pour en savoir plus sur le type utilisé pour chaque fonctionnalité, consultez Types de certificats utilisés par fonctionnalité, à la page 158.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de certificat lors de la modification d'une propriété de certificat en cliquant sur le lien **Create New Certificate** (Créer un certificat) affiché dans la liste des objets.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Certificates** (certificats) dans la table des matières.

Le système est livré avec les certificats prédéfinis suivants, que vous pouvez utiliser tels quels ou remplacer.

- DefaultInternalCertificate
- DefaultWebserverCertificate
- NGFW-Default-InternalCA

Le système comprend également de nombreux certificats d'autorité de certification de confiance provenant d'autorités de certification tierces. Ceux-ci sont utilisés par les politiques de déchiffrement SSL pour les actions de déchiffrement et de réauthentification. Le groupe Cisco-Trusted-Authorities comprend tous ces certificats et est le groupe par défaut utilisé par la politique de déchiffrement SSL.

Vous pouvez cliquer sur les filtres de recherche prédéfinis pour limiter la liste aux certificats **System-defined (définis par le système)** ou **User-defined** (définis par l'utilisateur).

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un nouvel objet de certificat, utilisez la commande pour le type de certificat dans le menu **+**.
- Pour créer un groupe de certificats, cliquez sur  et sélectionnez **Add Certificate Group** (Ajouter un groupe de certificats).
- Pour afficher ou modifier un certificat ou groupe, cliquez soit sur l'icône de modification () soit sur l'icône d'affichage () du certificat.
- Pour supprimer un certificat ou groupe non référencé, cliquez sur l'icône de la corbeille () du certificat.

Pour des informations détaillées sur la création ou la modification de certificats, consultez les rubriques suivantes :

- Charger les certificats d'identité interne et d'autorité de certification interne, à la page 161
- Génération de certificats internes autosignés et de certificats d'autorité de certification internes, à la page 163
- Téléchargement des certificats de l'autorité de certification de confiance, à la page 165
- Configuration des groupes de certificats CA de confiance, à la page 166

Charger les certificats d'identité interne et d'autorité de certification interne

Les certificats d'identité internes sont des certificats pour des systèmes ou des hôtes spécifiques.

Les certificats d'autorité de certification internes sont des certificats que le système peut utiliser pour signer d'autres certificats. Ces certificats varient des certificats d'identité internes en ce qui concerne l'extension des

contraintes de base et l'indicateur de l'autorité de certification, qui sont activés pour les certificats d'autorité de certification mais désactivés pour les certificats d'identité.

Vous pouvez générer ces certificats vous-même à l'aide de la boîte à outils OpenSSL ou les obtenir auprès d'une autorité de certification, puis les télécharger en utilisant la procédure suivante. Pour obtenir un exemple de génération d'une clé, consultez Exemple : génération d'un certificat interne à l'aide d'OpenSSL, à la page 159.

Vous pouvez également générer des certificats d'identité interne et d'autorité de certification interne autosignés. Si vous configurez des certificats d'autorité de certification internes autosignés, l'autorité de certification s'exécute sur le périphérique lui-même. Pour en savoir plus sur la création de certificats autosignés, consultez Génération de certificats internes autosignés et de certificats d'autorité de certification internes, à la page 163.

Pour en savoir plus sur les fonctionnalités qui utilisent ces certificats, consultez Types de certificats utilisés par fonctionnalité, à la page 158.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Certificates** (certificats) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur + > **Add Internal Certificate** (Ajouter un certificat interne), puis cliquez sur **Upload Certificate and Key** (Charger le certificat et la clé).
- Cliquez sur + > **Add Internal CA Certificate** (Ajouter un certificat d'autorité de certification interne), puis cliquez sur **Upload Certificate and Key** (Charger le certificat et la clé).
- Pour modifier ou afficher un certificat, cliquez sur l'icône d'information (). La boîte de dialogue affiche le sujet du certificat, l'émetteur et la période de validité. Cliquez sur Replace Certificate (Remplacer le certificat) pour charger un nouveau certificat et une nouvelle clé. Vous pouvez également coller le certificat et la clé dans la boîte de dialogue.

Étape 3 Entrez un nom (**Name**) pour le certificat.

Le nom est utilisé dans la configuration uniquement comme nom d'objet, il ne fait pas partie du certificat lui-même.

Étape 4 Cliquez sur **Upload Certificate** (Charger le certificat) (ou **Replace Certificate** (Remplacer le certificat) lors de la modification) et sélectionnez le fichier de certificat (par exemple, *.crt). Les extensions de fichier autorisées sont.pem, .cert, .cer, .crt et .der. Vous pouvez également coller le certificat.

Le certificat doit être un certificat X509 au format PEM ou DER.

Le certificat que vous collez doit inclure les lignes BEGIN CERTIFICATE et END CERTIFICATE. Par exemple :

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
```

```
-----END CERTIFICATE-----
```

Étape 5 Cliquez sur **Upload Key** (Charger la clé) (ou **Replace Key** (Remplacer la clé) lors de la modification) et sélectionnez le fichier de certificat (par exemple, *.key). L'extension du fichier doit être .key. Vous pouvez également coller la clé pour le certificat.

La clé ne peut pas être chiffrée et elle doit être une clé RSA.

Par exemple :

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQClSu1BknrMjzw/5FZ9YgdMLDUGJlbYgkjN7mVrkjyLQx2TYsem
r8iTiKB6iyTKbuS4iPeyEYkNF5FglCqKWEdmthNZkBhOsPs1A8e60r5mImeDrtw+
Cc0O5cSfnlTAw5CgcGkcxTCaGIZmXMkzwGlfYmzbJDeazfSmvys76A8I8wIDAQAB
AoGAUVDgEX8vXE0m9cOubPZ54pZo64KW/OJzUKP0TwxdLqGw/h39XFpkEXiIgmDL
(...5 lines removed...)
DSWvzekRDH83dmP66+MIbWePhbhty+D1OxbiuVuHV0/ZhxOhCG8tig3R8QJBAJmj
fId05+1dNI4tGbWv6hHh/H/dTP2STlZ3jERMZd29fjIRuJ9jpFC2lIDjvs8YGeAe
0YHkfSOULJn8/jOCf6kCQQDIJiHfGF/31Dk/8/5MGrg+3zau6oKXiuv6db8Rh+7l
MUOx09tvbBUy9REJq1YJWTKpeKD+E0QL+FX0bqvz4tHA
-----END RSA PRIVATE KEY-----
```

Étape 6 Cliquez sur **OK**.

Génération de certificats internes autosignés et de certificats d'autorité de certification internes

Les certificats d'identité internes sont des certificats pour des systèmes ou des hôtes spécifiques.

Les certificats d'autorité de certification internes sont des certificats que le système peut utiliser pour signer d'autres certificats. Ces certificats varient des certificats d'identité internes en ce qui concerne l'extension des contraintes de base et l'indicateur de l'autorité de certification, qui sont activés pour les certificats d'autorité de certification mais désactivés pour les certificats d'identité.

Vous pouvez générer un certificat d'identité interne autosigné et des certificats d'autorité de certification internes ; autrement dit, les certificats sont signés par le périphérique lui-même. Si vous configurez des certificats d'autorité de certification internes autosignés, l'autorité de certification s'exécute sur le périphérique. Le système génère le certificat et la clé.

Vous pouvez également créer ces certificats à l'aide d'OpenSSL ou les obtenir d'une autorité de certification de confiance et les téléverser. Pour en savoir plus, consultez Charger les certificats d'identité interne et d'autorité de certification interne, à la page 161.

Pour en savoir plus sur les fonctionnalités qui utilisent ces certificats, consultez Types de certificats utilisés par fonctionnalité, à la page 158.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Certificates** (certificats) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **+** > **Add Internal Certificate** (Ajouter un certificat interne), puis sur **Signed Certificate** (Certificat autosigné).
- Cliquez sur **+** > **Add Internal CA Certificate** (Ajouter un certificat d'autorité de certification interne), puis sur **Certificat autosigné**.

Remarque

Pour modifier ou afficher un certificat, cliquez sur l'icône d'information ( ). La boîte de dialogue affiche le sujet du certificat, l'émetteur et la période de validité. Cliquez sur **Replace Certificate** (Remplacer le certificat) pour charger un nouveau certificat et une nouvelle clé. Lors du remplacement d'un certificat, vous ne pouvez pas rétablir les caractéristiques d'autosignature expliquées dans les étapes suivantes. Au lieu de cela, vous devez coller ou charger un nouveau certificat, comme décrit dans Charger les certificats d'identité interne et d'autorité de certification interne, à la page 161. Les étapes restantes s'appliquent uniquement aux nouveaux certificats autosignés.

Étape 3 Entrez un nom (**Name**) pour le certificat.

Le nom est utilisé dans la configuration uniquement comme nom d'objet, il ne fait pas partie du certificat lui-même.

Étape 4 Configurez au moins l'un des éléments suivants pour les informations sur le sujet et l'émetteur du certificat.

- **Pays (C)** : le code du pays ISO 3166 à deux lettres à inclure dans le certificat. Par exemple, le code du pays pour les États-Unis est US. Sélectionnez le code du pays dans la liste déroulante.
- **État ou Province (ST)** : l'état ou la province à inclure dans le certificat.
- **Localité ou Ville (L)** : la localité à inclure dans le certificat, par exemple le nom de la ville.
- **Organisation (O)** : le nom de l'organisation ou de l'entreprise à inclure dans le certificat.
- **Unité organisationnelle (OU)** : le nom de l'unité organisationnelle (par exemple, le nom du service) à inclure dans le certificat.
- **Nom commun (CN)** : le nom commun X.500 à inclure dans le certificat. Il peut s'agir du nom du périphérique, du site Web ou d'une autre chaîne de texte. Cet élément est généralement requis pour la réussite des connexions. Par exemple, vous devez inclure un numéro de référence dans le certificat interne utilisé pour le VPN d'accès à distance.
- **Période de validité** : durée pendant laquelle le certificat sera considéré comme valide. La valeur par défaut est de 825 jours à compter d'aujourd'hui, quelle que soit la façon dont vous définissez la date d'expiration. Cliquez sur **Set default** (Rétablir les valeurs par défaut) pour revenir aux valeurs par défaut. Vous pouvez configurer la période à l'aide de l'une des méthodes suivantes. Veillez à remplacer les certificats avant leur expiration.
  - **By Date** (Par date) : cliquez sur **Expiration Date** (Date d'expiration) et sélectionnez le dernier jour où le certificat doit être considéré comme valide.
  - **By Number of Days** (Par nombre de jours) : saisissez le nombre de jours, à compter d'aujourd'hui, pendant lesquels le certificat doit être considéré comme valide. Après avoir saisi le nombre, vous pouvez cliquer sur **By Date (Par date)** pour voir la date d'expiration calculée.

Étape 5 Cliquez sur **Save** (Enregistrer).

Téléchargement des certificats de l'autorité de certification de confiance

Un certificat d'une autorité de certification de confiance (CA) est utilisé pour signer d'autres certificats. Il est autosigné et appelé certificat racine. Un certificat émis par un autre certificat CA s'appelle un certificat subordonné.

Pour en savoir plus sur les fonctionnalités qui utilisent ces certificats, consultez Types de certificats utilisés par fonctionnalité, à la page 158.

Obtenez un certificat d'autorité de certification de confiance auprès d'une autorité de certification externe ou créez-en un en utilisant votre propre autorité de certification interne, par exemple avec les outils OpenSSL. Ensuite, utilisez la procédure suivante pour télécharger le certificat.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Certificates** (certificats) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **+** > **Add Trusted CA Certificate** (ajouter un certificat d'autorité de certification de confiance).
- Pour modifier un certificat, cliquez sur l'icône de modification () du certificat.

Étape 3 Entrez un nom (**Name**) pour le certificat.

Le nom est utilisé dans la configuration uniquement comme nom d'objet, il ne fait pas partie du certificat lui-même.

Étape 4 Cliquez sur **Upload Certificate** (télécharger le certificat) (ou **Replace Certificate**, c.-à-d. remplacer le certificat lors de la modification) et sélectionnez le fichier de certificat d'autorité de certification (par exemple * .pem). Les extensions de fichier autorisées sont.pem, .cert, .cer, .crt et .der. Vous pouvez également coller le certificat d'autorité de certification de confiance.

Le nom du serveur dans le certificat doit correspondre au nom d'hôte/adresse IP du serveur. Par exemple, si vous utilisez 10.10.10.250 comme adresse IP mais ad.exemple.com dans le certificat, la connexion échouera.

Le certificat doit être un certificat X509 au format PEM ou DER.

Le certificat que vous collez doit inclure les lignes BEGIN CERTIFICATE et END CERTIFICATE. Par exemple :

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

Étape 5 Cliquez sur **OK**.

Configuration des groupes de certificats CA de confiance

Utilisez des groupes de certificats d'autorité de certification externes de confiance dans les paramètres de la politique de déchiffrement SSL pour préciser les certificats auxquels la politique de déchiffrement SSL doit faire confiance. Si un utilisateur final tente de se connecter à un site dont le certificat de l'émetteur ne fait pas partie des certificats de confiance, l'utilisateur reçoit un message lui demandant de faire confiance au certificat. Ainsi, le fait de ne pas avoir le certificat dans la liste de confiance est un inconvénient pour l'utilisateur final, mais n'empêche pas en soi la connexion (ce que vous pourriez faire avec des règles de contrôle d'accès).

Le groupe par défaut est Cisco-Trusted-Authorities. Vous ne devrez créer votre propre groupe que si :

- Vous souhaitez faire confiance aux certificats qui ne font pas partie du groupe par défaut. Vous devez ensuite sélectionner le groupe par défaut et votre nouveau groupe dans les paramètres de la politique de déchiffrement SSL.
- Vous souhaitez faire confiance à une liste de certificats plus limitée que le groupe par défaut. Vous devez ensuite créer un groupe qui a une liste complète de certificats de confiance, pas seulement votre delta, et le sélectionner comme seul groupe dans les paramètres de la politique de déchiffrement SSL.

Avant de commencer

Chargez tous les certificats d'autorités de certification de confiance que vous ajouterez au groupe, s'ils ne sont pas déjà présents dans le système.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Certificates** (certificats) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un groupe de certificats, cliquez sur  et sélectionnez **Add Certificate Group** (Ajouter un groupe de certificats).
- Pour modifier un groupe de certificats, cliquez sur l'icône de modification () du groupe.

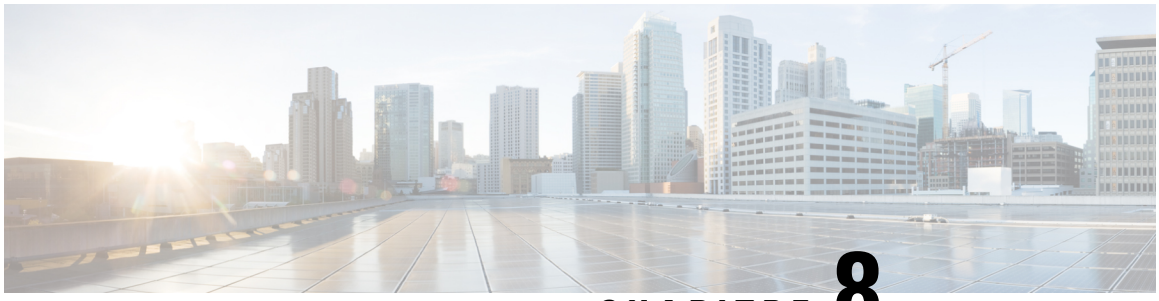
Étape 3 Entrez un **Name** (Nom) pour le groupe de certificats et, au besoin, une description.

Étape 4 Cliquez sur le signe **+** pour ajouter des certificats au groupe.

Ajoutez tous les certificats dont vous avez besoin dans le groupe. Vous pouvez cliquer sur **Create New Trusted CA Certificate** (Créer un nouveau certificat d'AC approuvée) pour en charger de nouveaux pendant que vous créez le groupe.

Si vous n'avez plus besoin d'un certificat dans le groupe, cliquez sur l'icône X (à droite) pour le certificat.

Étape 5 Cliquez sur **OK**.



CHAPITRE 8

Sources d'identité

Les sources d’identité sont des serveurs et des bases de données qui définissent les comptes utilisateur. Vous pouvez utiliser ces informations de diverses manières, par exemple pour fournir l’identité de l’utilisateur associée à une adresse IP ou authentifier des connexions VPN d’accès à distance ou l’accès à FDM.

Les rubriques suivantes expliquent comment définir les sources d'identité. Vous utiliserez ensuite ces objets lors de la configuration des services qui nécessitent une source d’identité.

- À propos des sources d’identité, à la page 167
- Domaine d’identité Active Directory (AD), à la page 169
- Serveurs et groupes RADIUS, à la page 176
- Identity Services Engine (ISE), à la page 180
- Serveurs SAML, à la page 184
- Utilisateurs locaux, à la page 186

À propos des sources d’identité

Les sources d’identité sont les serveurs et bases de données AAA qui définissent les comptes utilisateur pour les membres de votre organisation. Vous pouvez utiliser ces informations de diverses manières, par exemple en fournissant l’identité de l’utilisateur associée à une adresse IP, ou pour l’authentification des connexions VPN d’accès à distance ou de l’accès à Gestionnaire de périphériques de pare-feu.

Utilisez la page **Objects (Objects)** > **Identity Sources (Sources d’identité)** pour créer et gérer vos sources. Vous utiliserez ensuite ces objets lors de la configuration des services qui nécessitent une source d’identité.

Voici les sources d’identité prises en charge et leurs utilisations :

Domaine d’identité Active Directory (AD)

Active Directory fournit des informations sur le compte d’utilisateur et l’authentification. Consultez Domaine d’identité Active Directory (AD), à la page 169.

Vous pouvez utiliser cette source aux fins suivantes :

- Le VPN d’accès à distance, comme source d’identité principale. Vous pouvez utiliser AD conjointement avec un serveur RADIUS.
- Politique d’identité, pour l’authentification active et comme source d’identité d’utilisateur utilisée avec l’authentification passive.

Séquence de domaine AD (Active Directory)

Une séquence de domaine AD est une liste ordonnée d'objets de domaine AD. Les séquences de domaine sont utiles si vous gérez plusieurs domaines AD dans votre réseau. Consultez Configuration d'une séquence de domaine AD, à la page 173.

Vous pouvez utiliser cette source aux fins suivantes :

- Identity policy (stratégie d'identité), en tant que source d'identité d'utilisateur utilisée avec l'authentification passive. L'ordre des domaines dans la séquence détermine la façon dont le système détermine l'identité de l'utilisateur dans les rares cas de conflit.

Cisco Identity Services Engine (ISE) ou Cisco Identity Services Engine Passive Identity Connector (ISE PIC)

Si vous utilisez ISE, vous pouvez intégrer le périphérique Firepower Threat Defense à votre déploiement ISE. Consultez Identity Services Engine (ISE), à la page 180.

Vous pouvez utiliser cette source aux fins suivantes :

- Identity policy (stratégie d'identité), en tant que source d'identité passive pour collecter l'identité de l'utilisateur auprès d'ISE.

Serveurs RADIUS, Groupes de serveurs RADIUS

Si vous utilisez des serveurs RADIUS, vous pouvez également les utiliser avec le FDM. Vous devez définir chaque serveur comme un objet distinct, puis les placer dans des groupes de serveurs (où les serveurs d'un groupe donné sont des copies les uns des autres). Vous affectez le groupe de serveurs à des fonctionnalités, vous n'affectez pas de serveurs individuels. Consultez Serveurs et groupes RADIUS, à la page 176.

Vous pouvez utiliser cette source aux fins suivantes :

- Le VPN d'accès à distance, en tant que source d'identité pour l'authentification, et pour l'autorisation et la comptabilité. Vous pouvez utiliser AD conjointement avec un serveur RADIUS.
- La politique d'identité, en tant que source d'identité passive pour collecter l'identité de l'utilisateur à partir des connexions VPN d'accès à distance.
- Authentification extérieure pour les utilisateurs Gestionnaire de périphériques de pare-feu ou Firepower Threat Defense de gestion de l'interface de ligne de commande. Vous pouvez prendre en charge plusieurs utilisateurs de gestion avec différents niveaux d'autorisation. Ces utilisateurs peuvent se connecter au système à des fins de configuration et de surveillance des périphériques.

Serveur SAML

Security Assertion Markup Language 2.0 (SAML 2.0) est une norme ouverte pour l'échange de données d'authentification et d'autorisation entre les parties, en particulier un fournisseur d'identité (IdP) et un fournisseur de services (SP).

Vous pouvez utiliser cette source aux fins suivantes :

- VPN d'accès à distance, en tant que source d'authentification de connexion unique (SSO).

Source d'identité locale

Il s'agit de la base de données des utilisateurs locaux, qui comprend les utilisateurs que vous avez définis dans le FDM. Sélectionnez **Objects (Objets)** > **Users (Utilisateurs)** pour gérer les comptes d'utilisateurs dans cette base de données. Consultez Utilisateurs locaux, à la page 186.

Remarque La base de données de la source d'identité locale n'inclut pas les utilisateurs que vous configurez dans l'interface de ligne de commande pour l'accès à l'interface de ligne de commande (à l'aide de la commande **configure user add**). Les utilisateurs de l'interface de ligne de commande sont totalement distincts de ceux que vous créez dans le FDM.

Vous pouvez utiliser cette source aux fins suivantes :

- VPN d'accès à distance, comme source d'identité principale ou de secours.
- Politique d'identité, en tant que source d'identité passive pour collecter l'identité de l'utilisateur à partir des connexions VPN d'accès à distance.

Domaine d'identité Active Directory (AD)

Microsoft Active Directory (AD) définit les comptes utilisateur. Vous pouvez créer un domaine d'identité AD pour un domaine Active Directory. Les rubriques suivantes expliquent comment définir un domaine d'identité AD.

Serveurs d'annuaire pris en charge

Vous pouvez utiliser Microsoft Active Directory (AD) sur Windows Server 2012, 2016 et 2019.

Tenez compte des éléments suivants concernant la configuration de votre serveur :

- Si vous souhaitez effectuer un contrôle utilisateur sur des groupes d'utilisateurs ou sur les utilisateurs de groupes, vous devez configurer les groupes d'utilisateurs sur le serveur d'annuaire. Le système ne peut pas effectuer le contrôle des groupes d'utilisateurs si le serveur organise les utilisateurs selon une hiérarchie d'objets de base.
- Le serveur d'annuaire doit utiliser les noms de champ répertoriés dans le tableau suivant pour que le système puisse récupérer les métadonnées utilisateur des serveurs pour ce champ :

Métadonnées	Champ Active Directory
Nom d'utilisateur LDAP	samaccountname
prénom	prénom
nom	sn
adresse courriel	mail userprincipalname (si courriel n'a aucune valeur)
department	department distinguishedname (si le service n'a aucune valeur)
nom distinctif	telephonenumber

Limites relatives au nombre d'utilisateurs

FDM peut télécharger des informations sur un maximum de 50,000 utilisateurs à partir du serveur d'annuaire.

Si votre serveur d'annuaire comprend plus de 50 000 comptes utilisateur, vous ne verrez pas tous les noms possibles lors de la sélection des utilisateurs dans une règle d'accès ou lors de l'affichage des informations de tableau de bord basé sur l'utilisateur. Vous pouvez écrire des règles uniquement sur les noms qui ont été téléchargés.

La limite s'applique également aux noms associés aux groupes. Si un groupe compte plus de 50 000 membres, seuls les noms des 50 000 téléchargés peuvent être associés à l'appartenance au groupe.

Remarque Secure Firewall 200 peut télécharger un total cumulé de 10 000 adresses IP d'utilisateurs, mappages SXP/SGT, profils de points terminaux et objets dynamiques. Après un total de 10 000 téléchargés, l'appareil arrête de télécharger tous les objets jusqu'à ce que certains objets téléchargés précédemment aient été supprimés. (Par exemple, si les utilisateurs se déconnectent, la mémoire est libre pour d'autres objets.)

Détermination du DN de base du répertoire

Lorsque vous configurez les propriétés d'annuaire, vous devez préciser le nom distinctif (DN) commun de base pour les utilisateurs et les groupes. La base est définie dans votre serveur d'annuaire et diffère d'un réseau à l'autre. Vous devez entrer les bases avec exactitude pour que les politiques d'identité fonctionnent. Si la base est incorrecte, le système ne peut pas déterminer les noms d'utilisateur ou de groupe, de sorte que les politiques basées sur l'identité seront inutilisables.

Astuces Pour obtenir les bonnes bases, consultez l'administrateur responsable des serveurs d'annuaire.

Pour le répertoire actif (Active Directory), vous pouvez déterminer les bases exactes en vous connectant au serveur Active Directory en tant qu'administrateur de domaine et en utilisant la commande **dsquery** à l'invite de commande pour déterminer les bases. Voici la marche à suivre :

Point de départ de la recherche selon l'utilisateur

Entrez la commande **dsquery user** avec un nom d'utilisateur connu (partiel ou complet) pour déterminer le nom distinctif de base. Par exemple, la commande suivante utilise le nom partiel « John* » pour obtenir des informations pour tous les utilisateurs commençant par « John ».

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

Le DN de base serait « DC=csc-lab,DC=example,DC=com ».

Point de départ de la recherche selon le groupe

Entrez la commande **dsquery group** avec un nom de groupe connu pour déterminer le nom distinctif de base. Par exemple, la commande suivante utilise le nom de groupe « Employees » pour obtenir le nom distinctif :

```
C:\>dsquery group -name "Employees"
```

```
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

Le DN de base du groupe serait « DC=csc-lab,DC=example,DC=com ».

Vous pouvez également utiliser le programme ADSI Edit pour parcourir la structure Active Directory (**Start (démarrer)** > **Run (exécuter)** > **adsiedit.msc**). Dans ADSI Edit, cliquez avec le bouton droit de la souris sur n'importe quel objet, comme une unité organisationnelle, un groupe ou un utilisateur, puis choisissez **Properties** (propriétés) pour afficher le nom distinctif. Vous pouvez ensuite copier la chaîne de valeurs DC comme base.

Pour vérifier que vous avez établi la bonne base :

1. Sous les propriétés du répertoire, cliquez sur le bouton Test Connection (tester la connexion) pour vérifier la connectivité. Réglez les problèmes (le cas échéant) et enregistrez les propriétés du répertoire.
2. Validez les modifications apportées à l'appareil.
3. Créez une règle d'accès, sélectionnez l'onglet **Users** (utilisateurs) et essayez d'ajouter des noms d'utilisateur et de groupe connus à partir du répertoire. Vous devriez voir des suggestions automatiques lorsque vous tapez des entrées pour les utilisateurs et les groupes dans le domaine qui contient le répertoire. Si les suggestions apparaissent dans une liste déroulante, le système a pu interroger le répertoire avec succès. Si vous ne voyez aucune suggestion et que vous êtes certain que la chaîne que vous avez saisie doit apparaître dans un nom d'utilisateur ou de groupe, vous devez corriger le point de départ de la recherche en conséquence.

Configuration des domaines d'identité AD

Un domaine d'identité est un serveur de répertoire ainsi que d'autres attributs requis pour fournir des services d'authentification. Le serveur de répertoire contient des renseignements sur les utilisateurs et les groupes d'utilisateurs qui sont autorisés à accéder à votre réseau.

Pour Active Directory, un domaine équivaut à un domaine Active Directory. Créez des domaines distincts pour chaque domaine AD que vous devez prendre en charge.

Les domaines d'identité sont utilisés dans les politiques suivantes :

- Identité : le domaine d'identité fournit des informations sur l'identité de l'utilisateur et l'appartenance au groupe, que vous pouvez ensuite utiliser dans les règles de contrôle d'accès. Le système télécharge chaque jour les informations mises à jour sur tous les utilisateurs et groupes pendant la dernière heure du jour (UTC). Le serveur de répertoire doit être accessible à partir de l'interface de gestion.
- VPN d'accès à distance : le domaine d'identité fournit des services d'authentification, qui déterminent si une connexion est autorisée. Le serveur de répertoire doit être accessible à partir de l'interface externe du VPN d'accès à distance.
- Contrôle d'accès, déchiffrement SSL : vous pouvez sélectionner le domaine d'identité dans les critères utilisateur pour appliquer la règle à tous les utilisateurs du domaine.

Collaborez avec votre administrateur de répertoire pour obtenir les valeurs requises pour configurer les propriétés du serveur de répertoire.

Remarque Si le serveur de répertoire ne se trouve pas sur un réseau associé ou n'est pas disponible via la route par défaut, créez une route statique pour le serveur. Sélectionnez **Device (Périphérique)** > **Routing (Routage)** > **View Configuration (Afficher la configuration)** pour créer des routes statiques.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de domaine d'identité lorsque vous modifiez une propriété de domaine, en cliquant sur le lien **Create New Identity Realm** (Créer un nouveau domaine d'identité) affiché dans la liste d'objets.

Avant de commencer

Vérifiez que les paramètres d'horloge sont uniformes pour les serveurs d'annuaire, le périphérique Firewall Threat Defense et les clients. Un décalage temporel entre ces périphériques peut empêcher l'authentification de l'utilisateur réussie. « cohérence » signifie que vous pouvez utiliser différents fuseaux horaires, mais que l'heure doit être la même pour ces fuseaux horaires; par exemple, 10 h HNP = 13 h HNE.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez (Domaine d'identité) **Identity Sources** (Sources d'identité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un domaine AD, cliquez sur **+** > **AD**.
- Pour modifier un domaine, cliquez sur l'icône de modification ( ) du domaine.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés de base du domaine.

- **Name** (nom) : Nom du domaine de répertoire.
- **Type** : Type de serveur d'annuaire. Active Directory est le seul type pris en charge et vous ne pouvez pas modifier ce champ.
- **Directory Username** (nom d'utilisateur), **Directory Password** (mot de passe d'annuaire) : nom d'utilisateur et mot de passe uniques pour un utilisateur disposant des droits appropriés sur les informations utilisateur que vous souhaitez récupérer. Pour Active Directory, l'utilisateur n'a pas besoin d'avoir des privilèges élevés. Vous pouvez préciser n'importe quel utilisateur dans le domaine. Le nom d'utilisateur doit être complet; par exemple, Administrateur@exemple.com (pas simplement Administrateur).

  Remarque
  Le système génère ldap-login-dn et ldap-login-password à partir de ces informations. Par exemple, Administrateur@exemple.com se traduit par cn=administrator,cn=users,dc=example,dc=com. Notez que cn=users fait toujours partie de cette traduction; vous devez donc configurer l'utilisateur que vous précisez ici sous le nom usuel du dossier « users ».

- **Base DN** (base DN) : L'arborescence pour faire des recherches ou requêtes d'informations sur les utilisateurs et les groupes, c'est-à-dire le parent commun des utilisateurs et des groupes. Par exemple, cn=users,dc=example,dc=com. Pour en savoir plus sur la recherche du DN de base, consultez Détermination du DN de base du répertoire, à la page 170.
- **AD Primary Domain** (domaine principal AD) : le nom de domaine complet d'Active Directory que le périphérique doit joindre.' Par exemple, exemple.com.

Étape 4 Configurez les propriétés du serveur d'annuaire.

- **Hostname/IP Address** (nom d'hôte/adresse IP) : le nom d'hôte ou l'adresse IP du serveur d'annuaire. Si vous utilisez une connexion chiffrée avec le serveur, vous devez saisir le nom de domaine complet, et non l'adresse IP.
- **Port** : le numéro de port utilisé pour les communications avec le serveur. La valeur par défaut est 389. Utilisez le port 636 si vous sélectionnez LDAPS comme méthode de chiffrement.
- **Encryption** (chiffrement) : Pour utiliser une connexion chiffrée pour le téléchargement des informations sur les utilisateurs et les groupes, sélectionnez la méthode souhaitée, **STARTTLS** ou **LDAPS**. La valeur par défaut est **None** (aucun), ce qui signifie que les informations relatives aux utilisateurs et aux groupes sont téléchargées en texte en clair.
  - **STARTTLS** négocie la méthode de chiffrement et utilise la méthode la plus efficace prise en charge par le serveur d'annuaire. Utilisez le port 389. Cette option n'est pas prise en charge si vous utilisez le domaine pour le VPN d'accès à distance.
  - **LDAPS** nécessite LDAP sur SSL. Utilisez le port 636.
- **Trusted CA Certificate** (certificat CA de confiance) : Si vous sélectionnez une méthode de chiffrement, téléchargez un certificat d'autorité de certification (CA) pour activer une connexion de confiance entre le système et le serveur d'annuaire. Si vous utilisez un certificat pour vous authentifier, le nom du serveur dans le certificat doit correspondre au nom d'hôte ou à l'adresse IP du serveur. Par exemple, si vous utilisez 10.10.10.250 comme adresse IP mais ad.exemple.com dans le certificat, la connexion échouera.

Étape 5 S'il y a plusieurs serveurs pour le domaine, cliquez sur **Add Another Configuration** (Ajouter une autre configuration) et saisissez les propriétés de chaque serveur supplémentaire.

Vous pouvez ajouter jusqu'à 10 serveurs AD au domaine. Ces serveurs doivent être des doublons les uns des autres et prendre en charge le même domaine AD.

Vous pouvez réduire et développer chaque entrée de serveur pour votre commodité. Les sections sont étiquetées avec le nom d'hôte ou l'adresse IP et le port.

Étape 6 Cliquez sur le bouton **Test** (Tester) pour vérifier que le système peut communiquer avec le serveur.

Le système utilise des processus et des interfaces distincts pour accéder au serveur. Vous pourriez donc obtenir des erreurs indiquant que la connexion fonctionne pour un type d'utilisation mais pas pour un autre, par exemple, disponibles pour les politiques d'identité mais pas pour le VPN d'accès à distance. Si le serveur n'est pas accessible, vérifiez que vous avez la bonne adresse IP et le bon nom d'hôte, que le serveur DNS dispose d'une entrée pour le nom d'hôte, etc. Vous devrez peut-être configurer une route statique pour le serveur. Pour en savoir plus, consultez Résolution de problèmes liés aux connexions du serveur de répertoire, à la page 174.

Étape 7 Cliquez sur **OK**.

Configuration d'une séquence de domaine AD

Vous pouvez utiliser une séquence de domaine AD dans une règle d'identité passive afin que le système tente de faire correspondre les utilisateurs de plusieurs serveurs AD. Dans une séquence de domaine AD, vous configurez une liste ordonnée de domaines AD où chaque serveur AD gère un domaine différent, par exemple engineering.example.com et marketing.example.com.

Les séquences de domaine sont utiles uniquement si vous prenez en charge plusieurs domaines AD, et les utilisateurs de différents domaines peuvent envoyer le trafic par l'intermédiaire du périphérique Firewall Threat Defense. Les domaines sont utilisés pour trouver l'identité d'une session utilisateur authentifiée passivement. L'ordre des domaines est utilisé pour résoudre les conflits d'identité, dans les rares cas où un conflit pourrait survenir.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis **Identity Sources** (Sources d'identité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une séquence de domaine AD, cliquez sur **+** > **AD Realm Sequence** > **(+ Séquence de domaine AD)** .
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés de séquence de domaine :

- **Name** (Nom) : le nom de l'objet.
- **Description** : ajoutez une description facultative.
- **AD Realms** (Domaines AD) : cliquez sur le signe **+** pour ajouter des objets de domaine AD à la séquence. Après avoir ajouté les domaines, cliquez sur et faites glisser et déposez les domaines dans la séquence ordonnée souhaitée.

Étape 4 Cliquez sur **OK**.

Vous pouvez maintenant sélectionner la séquence de domaine AD dans une règle d'identité passive.

Résolution de problèmes liés aux connexions du serveur de répertoire

Le système utilise différents processus pour communiquer avec votre serveur de répertoire en fonction de la fonctionnalité. Ainsi, une connexion pour les politiques d'identité peut fonctionner, alors qu'une connexion pour le VPN d'accès à distance peut échouer.

Ces processus utilisent différentes interfaces pour communiquer avec le serveur de répertoire. Vous devez assurer la connectivité à partir de ces interfaces.

- Interface de gestion, pour : les politiques d'identité.
- Interface de données, pour : le VPN d'accès à distance (interface externe).

Lorsque vous configurez le domaine d'identité, utilisez le bouton **Test** pour vérifier que la connexion peut fonctionner. Les messages de défaillance doivent indiquer la fonctionnalité qui présente des problèmes de connexion. Voici les problèmes généraux que vous pourriez rencontrer, selon les attributs d'authentification et la configuration du routage et de l'interface.

Problèmes d'authentification des utilisateurs de répertoire.

Si le problème est que le système n'a pas pu se connecter au serveur de répertoire en raison du nom d'utilisateur ou du mot de passe, assurez-vous que le nom et le mot de passe sont corrects et valides sur le serveur de répertoire. Pour Active Directory, l'utilisateur n'a pas besoin d'avoir des privilèges élevés. Vous pouvez préciser n'importe quel utilisateur dans le domaine. Le nom d'utilisateur doit être complet; par exemple, Administrateur@exemple.com (pas simplement Administrateur).

Le système génère également ldap-login-dn et ldap-login-password à partir des informations de nom d'utilisateur et de mot de passe. Par exemple, Administrateur@exemple.com se traduit par cn=administrator,cn=users,dc=example,dc=com. Notez que cn=users fait toujours partie de cette traduction; vous devez donc configurer l'utilisateur que vous précisez ici sous le nom usuel du dossier « users ».

Le serveur de répertoire est accessible par l'intermédiaire d'une interface de données.

Si le serveur de répertoire se trouve sur un réseau directement connecté à une interface de données (comme une interface GigabitEthernet) ou routable à partir d'un réseau directement connecté, vous devez vous assurer qu'une route existe entre l'interface de gestion virtuelle et le serveur de répertoire.

- L'utilisation de **data-interfaces** comme passerelle de gestion devrait permettre au routage de s'effectuer correctement.
- Si vous avez une passerelle explicite sur l'interface de gestion, ce routeur doit disposer d'une route vers le serveur de répertoire.
- Vous n'avez pas besoin de configurer une adresse IP sur l'interface de **diagnostic**, qui est l'interface physique utilisée par l'interface de gestion virtuelle. Toutefois, si vous configurez une adresse, ne configurez pas également une route statique (comme une route par défaut) qui redirigerait le trafic destiné au serveur de répertoire vers l'interface de diagnostic.
- S'il y a un routeur entre le réseau directement connecté et le réseau qui héberge le serveur de répertoire, configurez une route statique pour le serveur de répertoire dans (**Device (Périphérique)** > **Routing (Routage)**).
- Vérifiez que l'interface de données dispose de l'adresse IP et du masque de sous-réseau appropriés.

Le serveur de répertoire est accessible par l'intermédiaire de l'interface physique de gestion.

Si le serveur de répertoire se trouve sur le réseau directement connecté à l'interface physique de gestion (comme Management0/0) ou routable à partir de ce réseau, vous devez effectuer les opérations suivantes :

- Configurez une adresse IPv4 pour l'interface de gestion (dont le nom logique est **diagnostic**) dans **Device (Périphérique)** > **Interfaces**. L'adresse IP doit se trouver sur le même sous-réseau que l'adresse de gestion virtuelle (**Device (Périphérique)** > **System Settings (Paramètres du système)** > **Management Interface (Interface de gestion)**).
- S'il y a un routeur entre le serveur de répertoire et l'interface de gestion, configurez une route pour le serveur de répertoire dans **Device (Périphérique)** > **Routing (Routage)** pour l'interface **diagnostic**.
- Vérifiez que les interfaces de diagnostic et de gestion possèdent l'adresse IP et le masque de sous-réseau appropriés.

Le serveur de répertoire se trouve sur un réseau externe.

Si le serveur de répertoire se trouve sur un réseau situé de l'autre côté de l'interface externe (liaison ascendante), vous devrez peut-être configurer une connexion VPN de site à site. Pour la procédure détaillée, consultez Comment utiliser un serveur de répertoire sur un réseau externe avec le VPN d'accès à distance, à la page 757.

Serveurs et groupes RADIUS

Vous pouvez utiliser les serveurs RADIUS pour authentifier et autoriser les connexions VPN d'accès à distance, ainsi que le FDM et les utilisateurs d'administration de l'interface de ligne de commande Firepower Threat Defense. Par exemple, si vous utilisez également Moteur de services de vérification des identités de Cisco (ISE) et son serveur RADIUS, vous pouvez utiliser ce serveur avec la fonction FDM.

Lorsque vous configurez une fonctionnalité pour utiliser des serveurs RADIUS, vous sélectionnez un groupe RADIUS plutôt que des serveurs individuels. Un groupe RADIUS est un ensemble de serveurs RADIUS qui sont des copies les uns des autres. Si un groupe a plusieurs serveurs, ils forment une chaîne de serveurs de sauvegarde pour assurer la redondance au cas où un serveur deviendrait indisponible. Mais même si vous n'avez qu'un seul serveur, vous devez créer un groupe comptant un seul membre pour configurer la prise en charge de RADIUS pour une fonctionnalité.

Les rubriques suivantes expliquent comment configurer des serveurs et des groupes RADIUS, afin qu'ils puissent être utilisés dans les fonctionnalités prises en charge.

Configurer les serveurs RADIUS

Les serveurs RADIUS fournissent des services AAA (authentification, autorisation et comptabilité). Si vous utilisez des serveurs RADIUS pour authentifier et autoriser les utilisateurs, vous pouvez utiliser ces serveurs avec le FDM.

Après avoir créé des objets pour chacun de vos serveurs RADIUS, créez des groupes de serveurs RADIUS pour contenir chaque groupe de serveurs en double.

Avant de commencer

Si vous souhaitez configurer une liste de contrôle d'accès de redirection pour le VPN d'accès à distance, vous devez utiliser la console d'interface en ligne de commande Smart (Smart CLI) pour créer la liste de contrôle d'accès étendue avant de créer ou de modifier l'objet serveur. Vous ne pouvez pas créer la liste de contrôle d'accès lors de la modification de l'objet.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis **Identity Sources** (Sources d'identité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur **+** > **RADIUS Server** (Serveur RADIUS).
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés suivantes :

- **Name** (Nom) : le nom de l'objet. Il n'est pas nécessaire que cela corresponde à quoi que ce soit configuré sur le serveur.

- **Nom ou adresse IP du serveur** : nom d'hôte complet (FQDN) ou adresse IP du serveur. Par exemple, radius.example.com ou 10.100.10.10.
- **Authentication Port** (Port d'authentification) : le port sur lequel l'authentification et l'autorisation RADIUS sont effectuées. Par défaut, c'est 1812 .
- **Timeout** : la durée, de 1 à 300 secondes, pendant laquelle le système attend une réponse du serveur avant d'envoyer la demande au serveur suivant. La valeur par défaut est de 10 secondes. Si vous utilisez ce serveur comme source d'authentification secondaire pour le VPN d'accès à distance, par exemple, pour demander un jeton d'authentification, augmentez ce délai d'authentification à 60 secondes au moins. Cela donne le temps à l'utilisateur d'obtenir et de saisir le jeton.
- **Server Secret Key** (Clé secrète du serveur) : (Facultatif.) le code secret partagé qui est utilisé pour chiffrer les données entre le dispositif Firepower Threat Defenseet le serveur RADIUS. La clé est une chaîne de caractères alphanumériques sensible à la casse et composé de jusqu'à 64 caractères, espaces exclus. La clé doit commencer par un caractère alphanumérique ou un trait de soulignement et peut contenir les caractères spéciaux : $ - _ . + @. Cette chaîne de caractères doit correspondre à la clé configurée sur le serveur RADIUS. Si vous ne configurez pas de clé secrète, la connexion ne sera pas chiffrée.

Étape 4 (Facultatif) Si vous utilisez le serveur pour la configuration Change of Authorization du VPN d'accès à distance, vous pouvez cliquer sur le lien **RA VPN Only** (VPN d'accès à distance uniquement) et configurer les options suivantes.

- **ACL de redirection** : sélectionnez la liste de contrôle d'accès étendue à utiliser pour la liste de contrôle d'accès de redirection du VPN d'accès à distance. Créez ces listes de contrôle d'accès au moyen de l'objet Smart CLI **Extended Access List** (liste d'accès étendue Smart CLI) dans la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)** > **Smart CLI** > **Objects (Objets)**.

  L'objectif de la liste de contrôle d'accès de redirection est d'envoyer le trafic initial à Cisco Identity Services Engine (ISE) afin qu'ISE puisse évaluer la posture du client. La liste de contrôle d'accès doit envoyer le trafic HTTPS à ISE, mais pas le trafic déjà destiné à ISE ou le trafic dirigé vers un serveur DNS pour la résolution de nom. Pour obtenir un exemple, consultez Configurer Change of Authorization (modification d'autorisation) sur le périphérique Firewall Threat Defense, à la page 738.
- **Interface utilisée pour la connexion au serveur RADIUS** : quelle interface utiliser lors de la communication avec le serveur. Si vous sélectionnez **Résoudre par recherche de route**, le système utilise toujours la table de routage pour déterminer l'interface à utiliser. Si vous sélectionnez **Sélectionner manuellement l'interface**, le système utilisera toujours l'interface que vous sélectionnez.

  Si vous configurez la modification d'autorisation, vous devez sélectionner une interface spécifique pour que le système puisse activer correctement l'écouteur CoA sur celle-ci.

  Si le serveur se trouve sur le même réseau que l'adresse de gestion, ce qui signifie que vous sélectionnerez l'interface de diagnostic, vous devez également configurer une adresse IP sur l'interface de diagnostic. Il n'est pas suffisant d'avoir une adresse IP de gestion. Accédez à **Device (Périphérique)** > **Interfaces**, et configurez une adresse IP sur l'interface de diagnostic qui se trouve sur le même sous-réseau que l'adresse IP de gestion.

  Si vous utilisez également ce serveur pour l'accès administratif Gestionnaire de périphériques de pare-feu, cette interface est ignorée. Les tentatives d'accès administratif sont toujours authentifiées au moyen de l'adresse IP de gestion.

Étape 5 (Facultatif, lors de la modification de l'objet uniquement.) Cliquez sur **Test** pour vérifier si le système peut se connecter au serveur.

Vous êtes alors invité(e) à saisir un nom d'utilisateur et un mot de passe. Le test vérifie si le serveur peut être contacté et, si oui, que le nom d'utilisateur peut être authentifié.

Étape 6 Cliquez sur **OK**.

Configurer les groupes de serveurs RADIUS

Un groupe de serveurs RADIUS contient un ou plusieurs objets serveur RADIUS. Les serveurs d'un groupe doivent être des copies les uns des autres. Ces serveurs forment une chaîne de serveurs de sauvegarde, de sorte que si le premier serveur n'est pas disponible, le système peut essayer le serveur suivant dans la liste.

Lorsque vous configurez la prise en charge de RADIUS dans une fonctionnalité, vous devez sélectionner un groupe de serveurs. Ainsi, même si vous n'avez qu'un seul serveur RADIUS, vous devez créer un groupe de serveurs pour le contenir.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis **Identity Sources** (Sources d'identité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur **+** > **RADIUS Server Group** (Groupe de serveurs RADIUS).
- Pour modifier un objet, cliquez sur l'icône de modification () de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille () de l'objet.

Étape 3 Configurez les propriétés suivantes :

- **Name** (Nom) : le nom de l'objet. Cela ne doit pas correspondre à ce qui est configuré sur les serveurs.
- **Dead Time** (Temps mort) : les serveurs défaillants ne sont réactivés que lorsque tous les serveurs sont tombés en panne. Le temps mort est le temps d'attente, de 0 à 1440 minutes, après l'échec du dernier serveur avant la réactivation 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.
- **Maximum Failed Attempts** (Nombre maximal de tentatives échouées) : le nombre de transactions AAA échouées (c'est-à-dire de demandes ne recevant pas de réponse) envoyées à un serveur RADIUS du groupe avant d'essayer le serveur suivant. Vous pouvez spécifier de 1 à 5, et la valeur par défaut est 3. Lorsque le nombre maximal de tentatives ayant échoué est dépassé, le système marque le serveur comme ayant échoué.

  Pour une fonctionnalité donnée, si vous avez configuré une méthode de secours à l'aide de la base de données locale et qu'aucun serveur du groupe ne répond, 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 la durée du temps mort, 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.
- **Dynamic Authorization (Autorisation dynamique)** (pour VPN RA uniquement), **Port** : si ous activez les services d'autorisation dynamique ou de changement d'autorisation (CoA) RADIUS pour ce groupe

de serveurs RADIUS, le groupe sera enregistré pour les notifications CoA et écoutera sur le port indiqué les mises à jour de la politique CoA provenant du Cisco Identity Services Engine (ISE). Le port d'écoute par défaut est 1700, ou vous pouvez définir un port différent dans l'intervalle 1024 à 65535. Activez l'autorisation dynamique uniquement si vous utilisez ce groupe de serveurs dans un VPN d'accès à distance en conjonction avec l'ISE.

- **Realm that Supports the RADIUS Server** (Domaine qui prend en charge le serveur RADIUS) : si le serveur RADIUS est configuré pour utiliser un serveur AD afin d'authentifier les utilisateurs, sélectionnez le domaine AD qui spécifie le serveur AD utilisé avec ce serveur RADIUS. Si le domaine n'existe pas déjà, cliquez sur **Create New Identity Realm** (Créer un nouveau domaine d'identité au bas de la liste et configurez-le maintenant.
- **RADIUS Server list** (Liste des serveurs RADIUS : sélectionnez jusqu'à 16 objets serveur RADIUS qui définissent les serveurs du groupe. Ajoutez ces objets dans l'ordre de priorité. Le premier serveur de la liste est utilisé jusqu'à ce qu'il cesse de répondre. Après avoir ajouté les objets, vous pouvez faire glisser et déposer pour les réorganiser. Si l'objet n'existe pas encore, cliquez sur **Create New RADIUS Server** (Créer un nouveau serveur RADIUS) pour le créer maintenant.

  Vous pouvez également cliquer sur le lien **Test (Tester)** pour vérifier que le système peut se connecter au serveur. Vous êtes alors invité(e) à saisir un nom d'utilisateur et un mot de passe. Le test vérifie si le serveur peut être contacté et, si oui, que le nom d'utilisateur peut être authentifié.

Étape 4 (Facultatif) Cliquez sur le bouton **Test All Servers** (Tester tous les serveurs) pour vérifier la connectivité à chaque serveur du groupe.

Vous êtes alors invité(e) à saisir un nom d'utilisateur et un mot de passe. Le système vérifie si chaque serveur peut être contacté et si le nom d'utilisateur peut être authentifié sur chaque serveur.

Étape 5 Cliquez sur **OK**.

Dépannage des serveurs et groupes RADIUS

Voici quelques éléments que vous pouvez vérifier si l'autorisation extérieure ne fonctionne pas.

- Utilisez les boutons **Test** dans le serveur RADIUS et les objets de groupe de serveurs pour vérifier que les serveurs peuvent être contactés à partir du périphérique. Assurez-vous de sauvegarder les objets avant le test. Si le test échoue :
  - Veuillez comprendre que le test ne tient pas compte de l'interface configurée pour le serveur et utilise toujours l'interface de gestion. Le test devrait échouer si le serveur mandataire d'authentification RADIUS n'est pas configuré pour répondre aux demandes de l'adresse IP de gestion.
  - Vérifiez que vous saisissez une bonne combinaison nom d'utilisateur/mot de passe pendant le test. Vous devriez recevoir un message Bad Credentials (Mauvaises informations d'authentification) s'ils sont incorrects.
  - Vérifiez la clé secrète, le port et l'adresse IP du serveur. Si vous utilisez un nom d'hôte, vérifiez que le DNS est configuré pour l'interface de gestion. Envisagez la possibilité que la clé secrète ait été modifiée sur le serveur RADIUS, mais pas dans la configuration du périphérique.

- Si le test continue d'échouer, vous devrez peut-être configurer une voie de routage statique vers les serveurs RADIUS. Essayez d'envoyer un message Ping au serveur à partir de la console d'interface de ligne de commande ou d'une session SSH pour voir s'il est possible de le joindre.

- Si l'authentification externe fonctionnait mais a cessé de fonctionner, envisagez la possibilité que tous les serveurs soient dans la période de délai mort. Lorsque tous les serveurs RADIUS d'un groupe ont échoué, « dead time » (délai mort) correspond au nombre de minutes pendant lesquelles le système attend avant de réessayer le premier serveur. Pendant le temps mort, l'authentification locale est utilisée, de sorte que le nom d'utilisateur et le mot de passe d'un utilisateur donné seraient le nom d'utilisateur et le mot de passe locaux. La valeur par défaut est de 10 minutes, mais vous pouvez configurer jusqu'à 1 440 minutes.
- Si l'authentification externe HTTPS fonctionne pour certains utilisateurs mais pas pour d'autres, évaluez l'attribut cisco-av-pair défini dans le serveur RADIUS pour chaque compte d'utilisateur. Cet attribut est peut-être mal configuré. Un attribut manquant ou incorrect bloquera tout accès HTTPS pour ce compte d'utilisateur.
- Si l'authentification externe SSH fonctionne pour certains utilisateurs mais pas pour d'autres, évaluez l'attribut Service-Type défini dans le serveur RADIUS pour chaque compte d'utilisateur. Cet attribut est peut-être mal configuré. Un attribut manquant ou incorrect bloquera tout accès SSH pour ce compte d'utilisateur.

Identity Services Engine (ISE)

Vous pouvez intégrer votre déploiement de Cisco Identity Services Engine (ISE) ou de ISE Passive Identity Connector (ISE-PIC) au Firepower Threat Defense pour utiliser ISE/ISE-PIC pour l'authentification passive.

ISE/ISE-PIC est une source d'identité faisant autorité et fournit des données de connaissance des utilisateurs pour les utilisateurs qui s'authentifient à l'aide d'Active Directory (AD), LDAP, RADIUS ou RSA. Cependant, pour Firepower Threat Defense, vous pouvez utiliser ISE pour connaître l'identité des utilisateurs en conjonction avec AD uniquement. Vous pouvez utiliser l'identité de l'utilisateur dans les politiques de contrôle d'accès et de déchiffrement SSL comme critères de correspondance, en plus de voir les informations de l'utilisateur dans les différents tableaux de bord et événements de surveillance.

Pour en savoir plus sur Cisco ISE/ISE-PIC, consultez le *Guide de l'administrateur de services d'identité Cisco Identity Services Engine* (https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html) et le *Guide d'installation et d'administration d'Identity Services Engine Passive Identity Connector (ISE-PIC)* (https://www.cisco.com/c/en/us/support/security/ise-passive-identity-connector/tsd-products-support-series-home.html).

Lignes directrices et limites pour ISE

- Le système de pare-feu ne prend pas en charge l'authentification 802.1x des périphériques en parallèle de l'authentification Active Directory, parce qu'il n'associe pas l'authentification des périphériques aux utilisateurs. Si vous utilisez des connexions actives 802.1x, configurez ISE pour signaler uniquement les connexions actives 802.1x (périphérique et utilisateur). De cette façon, une connexion de périphérique n'est signalée qu'une seule fois au système.
- ISE/ISE-PIC ne signale pas l'activité des utilisateurs des services invités ISE.

- Synchronisez l'heure sur le serveur ISE/ISE-PIC et sur le périphérique. Sinon, le système pourrait provoquer des expirations de délai d'utilisateur à des intervalles inattendus.
- Si vous configurez l'ISE/ISE-PIC pour surveiller un grand nombre de groupes d'utilisateurs, le système pourrait abandonner les mappages d'utilisateurs en fonction des groupes en raison des limites de mémoire. Par conséquent, les règles assorties de conditions de domaine ou d'utilisateur peuvent ne pas fonctionner comme prévu.
- Pour connaître les versions précises d'ISE/ISE-PIC compatibles avec cette version du système, consultez le *Guide de compatibilité Cisco Secure Firewall*https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-device-support-tables-list.html,
- Utilisez l'adresse IPv4 du serveur ISE, sauf si vous confirmez que votre version d'ISE prend en charge IPv6.

Configurer Identity Services Engine (ISE)

Pour utiliser le moteur de services d'identité de Cisco (ISE) ou le connecteur d'identité passive du moteur de services d'identité de Cisco (ISE PIC) comme source d'identité passive, vous devez configurer la connexion au serveur ISE Platform Exchange Grid (pxGrid).

Avant de commencer

- Exportez les certificats de serveur pxGrid et MNT à partir d'ISE. Par exemple, dans ISE PIC 2.2, vous les trouvez sur la page **Certificates (Certificates)** > **Certificate Management (Gestion des certificats)** > **System Certificates (Certificats système)**. Le MNT (nœud de surveillance et de dépannage) est affiché comme Admin dans la colonne Utilisé par dans la liste des certificats. Vous pouvez soit les charger en tant que certificats d'autorité de certification de confiance sur la page **Objects (Objets)** > **Certificates (Certificats)**, soit les charger au cours de la procédure suivante. Ces nœuds peuvent utiliser le même certificat.
- Vous devez également configurer un domaine d'identité AD. Le système obtient la liste des utilisateurs d'AD et d'ISE il obtient des informations sur les mappages utilisateur-adresse IP.
- Si vous utilisez des balises de groupe de sécurité (SGT) pour le contrôle d'accès, avec ou sans mappages statiques de balises de groupe de sécurité, et si vous écoutez le sujet SXP, vous devez également configurer SXP et ces mappages dans ISE. Consultez Configurer les groupes de sécurité et la publication SXP dans ISE, à la page 535.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis **Identity Sources** (Sources d'identité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur **+** > **Identity Services Engine (Identity Services Engine)**. Vous pouvez créer au maximum un objet ISE.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés suivantes :

- **Name** (Nom) : le nom de l'objet.
- **Status** (État) : cliquez sur la bascule pour activer ou désactiver l'objet. Lorsque cette option est désactivée, vous ne pouvez pas utiliser ISE comme source d'identité dans vos règles d'identité.
- **Description** : ajoutez une description facultative.
- **Primary Node Hostname/IP Address** (Nom d'hôte/adresse IP du nœud principal) : nom d'hôte ou adresse IP du serveur ISE pxGrid principal. Ne spécifiez pas d'adresse IPv6, sauf si vous avez vérifié que votre version d'ISE prend en charge IPv6.
- **Secondary Node Hostname/IP Address** (Nom d'hôte/adresse IP du nœud secondaire) : si vous configurez un serveur ISE secondaire pour la haute disponibilité, cliquez sur **Add Secondary Node Hostname/IP Address** (Ajouter un nom d'hôte/adresse IP de nœud secondaire) et saisissez le nom d'hôte ou l'adresse IP du serveur ISE pxGrid secondaire.
- **pxGrid Server CA Certificat**e (Certificat CA du serveur pxGrid) : le certificat de l'autorité de certification de confiance pour le cadre pxGrid. Si votre déploiement comprend un nœud pxGrid principal et un nœud secondaire, les certificats des deux nœuds doivent être signés par la même autorité de certification.
- **MNT Server CA Certificat**e (Certificat CA du serveur MNT : le certificat de l'autorité de certification de confiance pour le certificat ISE lors des téléchargements en bloc. Il peut s'agir du même certificat que celui du serveur pxGrid si votre serveur MNT (surveillance et dépannage) n'est pas distinct. Si votre déploiement comprend un nœud MNT principal et un nœud secondaire, les certificats des deux nœuds doivent être signés par la même autorité de certification.
- **Server Certificate** (Certificat du serveur) : le certificat d'identité interne que le périphérique Firepower Threat Defense doit fournir à ISE lors de la connexion à ISE ou lors des téléchargements en bloc.
- **Subscribe To (S'abonner à) :** sélectionnez les rubriques ISE pxGrid auxquelles vous devez vous abonner. S'abonner à une rubrique signifie que vous téléchargerez les données liées à cette rubrique.
  - **Session Directory Topic** (Rubrique Session Directory) : indique s'il faut obtenir des informations sur les sessions utilisateur, y compris les mappages SGT pour ces sessions. Par défaut, cette option est activée. Vous devez sélectionner cette option si vous souhaitez obtenir une identité d'utilisateur passive à utiliser dans les politiques de sécurité et pour la visibilité dans les tableaux de bord de surveillance.
  - **SXP Topic** (Rubrique SXP) : indique s'il faut obtenir des mappages statiques SGT–adresses IP. Sélectionnez cette rubrique si vous souhaitez écrire des règles de contrôle d'accès en fonction des balises de groupe de sécurité (SGT).
- **ISE Network Filters** (Filtres de réseau ISE) : filtre facultatif que vous pouvez définir pour restreindre les données qu'ISE transmet au système. Si vous fournissez un filtre de réseau, ISE ne signale que les données provenant des réseaux inclus dans ce filtre. Cliquez sur **+**, sélectionnez les objets réseau qui identifient les réseaux, puis cliquez sur **OK**. Cliquez sur **Create New Network** (Créer un nouveau réseau) si vous devez créer les objets. Configurez uniquement les objets réseau IPv4.

Étape 4 Cliquez sur le bouton **Test** pour vérifier que le système peut se connecter à votre serveur ISE.

Si le test échoue, cliquez sur le lien **See Logs** (Voir les journaux) pour lire les messages d'erreur détaillés. Par exemple, le message suivant indique que le système n'a pas pu se connecter au serveur sur le port requis. Le problème peut provenir de l'absence de route vers l'hôte, du fait que le serveur ISE n'utilise pas le port attendu ou de règles de contrôle d'accès qui empêchent la connexion.

```
Captured Jabberwerx log:2018-05-11T16:10:30 [   ERROR]: connection timed out while
trying to test connection to host=10.88.127.142:ip=10.88.127.142:port=5222
```

Étape 5 Cliquez sur **OK** pour enregistrer l'objet.

Prochaine étape

Après avoir configuré ISE, activez la politique d'identité, configurez les règles d'authentification passive et déployez la configuration. Ensuite, vous devez accéder à ISE/ISE PIC et accepter le périphérique en tant qu'abonné. Si vous configurez ISE/ISE PIC pour accepter automatiquement les utilisateurs, vous n'avez pas besoin d'accepter manuellement l'abonnement.

Dépannage de la source d'identité ISE/ISE-PIC

Connexions ISE/ISE-PIC

Si vous rencontrez des problèmes avec la connexion ISE ou ISE-PIC, vérifiez les éléments suivants :

- La fonctionnalité de mappage d'identité pxGrid dans ISE doit être activée avant de pouvoir intégrer avec succès ISE au périphérique Firepower Threat Defense.
- Avant d'établir une connexion entre le serveur ISE et le périphérique Firepower Threat Defense, vous devez approuver manuellement les clients dans ISE.

  Vous pouvez également activer **Automatically approve new accounts** (Approuver automatiquement les nouveaux comptes) dans ISE, comme indiqué dans le chapitre sur la gestion des utilisateurs et des sources d'identité externes dans le *Guide de l'administrateur de Cisco Identity Services Engine*.
- Le certificat du périphérique Firepower Threat Defense (serveur) doit inclure la valeur d'utilisation de clé étendue **clientAuth** ou ne doit inclure aucune valeur d'utilisation de clé étendue. If the clientAuth extended key usage is set… Si l'utilisation de clé étendue clientAuth est définie, aucune utilisation de clé ne doit être définie, ou la valeur d'utilisation de la clé de signature numérique (Digital Signature) doit être définie. Les certificats d'identité autosignés que vous pouvez créer à l'aide du Gestionnaire de périphériques de pare-feu répondent à ces exigences.
- L'heure de votre serveur ISE doit être synchronisée avec l'heure sur le périphérique Firepower Threat Defense. Si les périphériques ne sont pas synchronisés, le système peut provoquer des délais d'expiration d'utilisateur à des intervalles imprévus.

Utilisateurs ISE/ISE-PIC

Si vous rencontrez des problèmes avec les données des utilisateurs signalées par ISE ou ISE-PIC, tenez compte des éléments suivants :

- Une fois que le système a détecté une activité d'un utilisateur ISE dont les données ne sont pas encore dans la base de données, le système récupère les informations à propos du serveur. L'activité vue par l'utilisateur ISE n'est pas gérée par les règles de contrôle d'accès et n'est pas affichée dans l'interface Web tant que le système n'a pas récupéré les informations la concernant lors d'un téléchargement d'utilisateur.

- Vous ne pouvez pas effectuer le contrôle utilisateur sur les utilisateurs ISE qui ont été authentifiés par un contrôleur de domaine LDAP, RADIUS ou RSA.
- Le système ne reçoit pas les données d'utilisateur pour les utilisateurs des services invités de Cisco ISE.

Serveurs SAML

Vous pouvez configurer les serveurs Security Assertion Markup Language 2.0 (SAML 2.0) pour les utiliser comme sources d'authentification par connexion unique (SSO) pour les connexions VPN d'accès à distance. SAML est une norme ouverte pour l'échange de données d'authentification et d'autorisation entre des parties, en particulier un fournisseur d'identité (IdP) et un fournisseur de services (SP).

Configurer les serveurs SAML

Vous pouvez configurer les serveurs Security Assertion Markup Language 2.0 (SAML 2.0) pour les utiliser comme sources d'authentification par connexion unique (SSO) pour les connexions VPN d'accès à distance. Par exemple, Duo Access Gateway (DAG) est un serveur SAML.

Lorsque vous utilisez un serveur SAML comme méthode d'authentification, le serveur SAML agit en tant que fournisseur d'identité (IdP), tandis que le périphérique Firewall Threat Defense agit en tant que fournisseur de services (SP).

Pour le VPN d'accès à distance, vous pouvez utiliser un serveur SAML comme source d'authentification principale, mais vous ne pouvez pas configurer une source d'authentification secondaire ni configurer une source de repli.

Avant de commencer

Obtenez les informations suivantes auprès du fournisseur d'identité du serveur SAML.

- URL de l'identifiant d'entité, qui fournit les métadonnées du serveur SAML.
- URL de connexion.
- URL de déconnexion.
- Certificat du fournisseur d'identité.

Le système ne prend pas en charge plusieurs valeurs renvoyées pour un attribut SAML. Par exemple, si vous utilisez SAML avec le VPN d'accès à distance, vous ne pouvez pas fournir plusieurs valeurs pour l'attribut de la politique de groupe Cisco : vous ne devez fournir qu'une seule valeur. Si vous envoyez plusieurs valeurs, une valeur par défaut est appliquée plutôt que de choisir l'une des valeurs fournies. Assurez-vous que le serveur SAML est configuré pour fournir une valeur unique pour chaque attribut renvoyé.

Procédure

Étape 1 Effectuez l'une des opérations suivantes pour accéder à la page des serveurs SAML :

- Sélectionnez **Objects** (Objets), puis **Identity Sources** (Sources d'identité) dans la table des matières.

- Sélectionnez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** > **SAML Servers (Serveurs SAML)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur **+** > **SAML Server** (Serveur SAML) .
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés suivantes :

- **Name** (Nom) : le nom de l'objet.
- **Description** : ajoutez une description facultative.
- **URL de l'identifiant d'entité du fournisseur d'identité (IDP)** : l'URL d'une page qui sert le XML de métadonnées qui décrit comment l'émetteur SAML répondra aux demandes. Certains produits de serveur SAML l'appellent l'ID d'entité, d'autres l'appellent l'URL de métadonnées. L'URL doit comporter de 4 à 128 caractères, y compris le protocole, https://. Par exemple, https://191.168.2.21/dag/saml2/idp/metadata.php.
- **Sign-In URL** (URL de connexion) : l'URL pour la connexion au serveur du fournisseur d'identité SAML. L'URL doit comporter de 4 à 500 caractères, y compris le protocole. http:// et https:// sont autorisés. Par exemple, https://191.168.2.21/dag/saml2/idp/SSOService.php.
- **Sign-Out URL** (URL de déconnexion) : l'URL pour la déconnexion du serveur du fournisseur d'identité SAML. L'URL doit comporter de 4 à 500 caractères, y compris le protocole. http:// et https:// sont autorisés. Par exemple, https://191.168.2.21/dag/saml2/idp/SingleLogoutService.php.
- **Service Provider Certificate** (Certificat du fournisseur de services) : le certificat interne à utiliser pour le périphérique Firewall Threat Defense. Idéalement, vous avez déjà chargé un certificat signé par un tiers reconnu et vous pouvez le sélectionner maintenant. Vous pouvez également utiliser le certificat intégré DefaultInternalCertificate (Certificat interne par défaut), ou cliquer sur **Create New Internal Certificate** (Créer un nouveau certificat interne) et charger un certificat signé maintenant. Le fournisseur d'identité du serveur SAML devra faire confiance à ce certificat, vous devrez peut-être le charger sur le serveur SAML. Consultez la documentation du serveur SAML pour obtenir des renseignements sur la façon de charger des certificats ou d'activer une relation de confiance avec un fournisseur de services.
- **Identity Provider Certificate** (Certificat du fournisseur d'identité) : certificat de l'autorité de certification de confiance pour le fournisseur d'identité du serveur SAML. Téléchargez ce certificat à partir du serveur SAML. Si vous ne l'avez pas encore chargé, cliquez sur **Create New Trusted CA Certificate** (Créer un nouveau certificat d'AC de confiance) et chargez-le maintenant.
- **Request Signature** (Signature de la demande) : l'algorithme de chiffrement à utiliser lors de la signature de la demande de connexion. Sélectionnez Aucun pour désactiver le chiffrement. Sinon, choisissez l'un des éléments suivants, qui sont classés du plus faible au plus fort : SHA1, SHA256, SHA384, SHA512.
- **Request Timeout** (Délai d'expiration de la demande) : les assertions SAML ont une période de validité : l'utilisateur doit finaliser la demande d'authentification unique (SSO) dans ce délai. Vous pouvez définir un délai d'expiration, en secondes, pour changer cette période. Si vous définissez un délai d'expiration plus long que la condition NotOnOrAfter de l'assertion, votre délai d'expiration est ignoré, et la condition NotOnOrAfter est respectée. La plage est de 1 à 7 200 secondes. La valeur par défaut est de 300 secondes.

- **This SAML identity provider (IDP) is on an internal network** (Ce fournisseur d'identité SAML est sur un réseau interne) : indique si le serveur SAML fonctionne sur un réseau interne plutôt qu'à l'extérieur des réseaux protégés.
- **Request IDP re-authentication at login** (Demander une réauthentification IdP à la connexion) : sélectionnez cette option pour obliger l'utilisateur à se réauthentifier à chaque connexion, au lieu de laisser le serveur SAML réutiliser une session d'authentification précédente. Par défaut, cette option est activée.

Étape 4 Cliquez sur **OK**.

Prochaine étape

Si vous avez activé la fonction **Request Signature** (Demande de signature) pour chiffrer les communications, vous devez charger les informations du gestionnaire d'appareil sur le serveur SAML. Dans la liste des sources d'identité, cliquez sur le bouton **Download** (Télécharger) ( ) pour le serveur et enregistrez le fichier XML. Ensuite, connectez-vous au serveur SAML et chargez les informations. Consultez la documentation de votre fournisseur SAML pour obtenir des informations détaillées.

Si vous utilisez le serveur pour la connexion au gestionnaire d'appareils et qu'il ne fonctionne pas, vérifiez la configuration du serveur SAML.

- Connectez-vous au fournisseur d'identité de SAML et vérifiez que le consommateur de réponses SAML du gestionnaire d'appareil est configuré correctement. La valeur doit être : https://<FDM_URL>/api/fdm/latest/fdm/token
- Si la Demande de signature est activée dans l'objet serveur SAML, assurez-vous que le certificat public du gestionnaire d'appareil est chargé dans l'application SAML et que le chiffrement est activé. Le chargement du fichier XML du gestionnaire d'appareil devrait ajouter le certificat au serveur SAML. Vous pouvez également récupérer le certificat du gestionnaire d'appareil par le biais de l'API FDM : https://<FDM_URL>/saml/metadata

Utilisateurs locaux

La base de données des utilisateurs locaux (LocalIdentitySource) comprend les utilisateurs que vous avez définis dans le FDM.

Vous pouvez utiliser des utilisateurs définis localement aux fins suivantes :

- Remote Access VPN (VPN d'accès à distance), en tant que source d'identité principale ou de secours.
- Management Access (Accès de gestion), en tant que source principale ou secondaire pour les utilisateurs FDM.

  L'utilisateur **admin** est un utilisateur défini localement par le système. Cependant, l'utilisateur admin ne peut pas se connecter à un VPN d'accès à distance. Vous ne pouvez pas créer d'utilisateurs administratifs locaux supplémentaires.

  Si vous définissez l'authentification extérieure pour l'accès de gestion, les utilisateurs externes qui se connectent au périphérique s'affichent dans la liste des utilisateurs locaux.

- Identity Policy (Politique d'identité), indirectement, en tant que source d'identité passive pour collecter l'identité des utilisateurs à partir des connexions VPN d'accès à distance.

Le sujet suivant explique comment configurer les utilisateurs locaux.

Configurer les utilisateurs locaux

Vous pouvez créer des comptes utilisateur directement sur le périphérique pour une utilisation avec le VPN d'accès à distance. Vous pouvez utiliser les comptes d'utilisateurs locaux au lieu ou en plus d'une source d'authentification externe.

Si vous utilisez la base de données d'utilisateurs locaux comme méthode d'authentification de repli pour le VPN d'accès à distance, veillez à configurer les mêmes noms d'utilisateur et mots de passe dans la base de données locale que les noms dans la base de données externe. Sinon, le mécanisme de repli ne sera pas efficace.

Les utilisateurs définis ici ne peuvent pas se connecter à l'interface de ligne de commande du périphérique.

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Users (Utilisateurs)**.

La liste affiche les noms d'utilisateurs et les types de services, qui peuvent être :

- MGMT : pour les utilisateurs administrateurs qui peuvent se connecter à Gestionnaire de périphériques de pare-feu. L'utilisateur admin est toujours défini et vous ne pouvez pas le supprimer. Vous ne pouvez pas non plus configurer d'utilisateurs MGMT supplémentaires. Toutefois, si vous définissez l'authentification extérieure pour l'accès de gestion, les utilisateurs externes qui se connectent au périphérique s'affichent dans la liste des utilisateurs locaux en tant qu'utilisateurs MGMT.
- VPN d'accès à distance : pour les utilisateurs qui peuvent se connecter à un VPN d'accès à distance configuré sur le périphérique. Vous devez également sélectionner la base de données locale pour la source principale ou secondaire (de repli).

Étape 2 Effectuez l'une des opérations suivantes :

- Pour ajouter un utilisateur, cliquez sur **+**.
- Pour modifier un utilisateur, cliquez sur l'icône de modification ( ) correspondant à l'utilisateur.

Si vous n'avez plus besoin d'un compte d'utilisateur particulier, cliquez sur l'icône de suppression ( ) pour l'utilisateur.

Étape 3 Configurez les propriétés de l'utilisateur :

Le nom et le mot de passe peuvent contenir n'importe quel caractère alphanumérique ou spécial ASCII imprimé, à l'exception des espaces et des points d'interrogation. Les caractères imprimés sont les codes ASCII 33 à 126.

- **Nom** : nom d'utilisateur pour la connexion au VPN d'accès à distance. Le nom peut comporter de 4 à 64 caractères et ne peut pas contenir d'espaces. Par exemple : jeanuntel.
- **Mot de passe** et **Confirmer le mot de passe** : Saisissez le mot de passe de l'utilisateur. Le mot de passe doit comporter de 8 à 16 caractères. Il ne peut pas contenir de lettres consécutives identiques. Il doit

également contenir au moins un des éléments suivants : un chiffre, une majuscule, une minuscule et un caractère spécial.

Remarque
Les utilisateurs ne peuvent pas modifier leur mot de passe. Avisez-les de leurs mots de passe et, lorsqu'ils doivent les modifier, vous devez modifier le compte d'utilisateur. De plus, ne mettez pas à jour le mot de passe des utilisateurs MGMT externes : les mots de passe sont contrôlés par le serveur AAA externe.

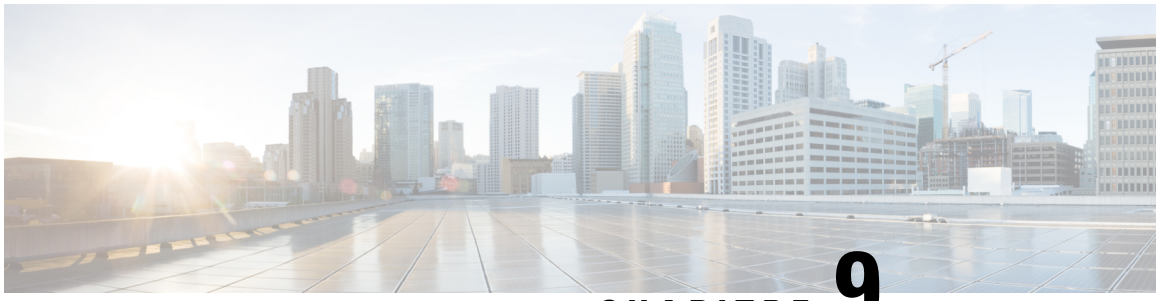
Étape 4 Cliquez sur **OK**.



PARTIE III

Principes de base

- Périphériques logiques sur les appareils Firepower 4100/9300, à la page 191
- Haute disponibilité (basculement), à la page 203
- Interfaces, à la page 251



CHAPITRE 9

Périphériques logiques sur les appareils Firepower 4100/9300

Firepower 4100/9300 est une plateforme de sécurité flexible sur laquelle vous pouvez installer un ou plusieurs *périphériques logiques*.

Vous devez configurer les interfaces de châssis, ajouter un périphérique logique et affecter des interfaces au périphérique sur le châssis Firepower 4100/9300 à l'aide de Cisco Firepower Chassis Manager ou de la CLI FXOS. Vous ne pouvez pas effectuer ces tâches dans Gestionnaire de périphériques de pare-feu.

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 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 191
- Exigences et conditions préalables pour les combinaisons matérielles et logicielles de l'appareil Firepower 9300, à la page 193
- Lignes directrices et limites relatives aux périphériques logiques, à la page 194
- Interfaces de configuration, à la page 195
- Configurer un périphérique logique, à la page 197
- Historique des dispositifs logiques Firepower 4100/9300, à la page 202

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 Firepower Chassis Manager. 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 (Firepower Threat Defense-utilisant-Centre de gestion Firepower (FMC) 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 191.

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 Firepower Threat Defense-using- (en usage) Centre de gestion Firepower (FMC).

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. Le Gestionnaire de périphériques de pare-feu et le Contrôle de Security Cloud ne prennent pas en charge la mise en grappe.

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.

Exigences et conditions préalables pour les combinaisons matérielles et logicielles de l'appareil 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.
- 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.

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

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 deux unités d'une configuration de basculement à haute accessibilité doivent :
  - 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.
- Pour en savoir plus, consultez Configuration requise pour la haute accessibilité, à la page 212.

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 .

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.

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 d'Actif à Activé.

Le Châssis Firepower 4100/9300 ne prend en charge les EtherChannels qu'en mode LACP actif de sorte que chaque interface membre envoie et reçoive des mises à jour 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.

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 Châssis 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**.

Configurer un périphérique logique

Ajoutez un périphérique logique autonome ou une paire à haute disponibilité sur Châssis Firepower 4100/9300 .

Ajouter un FTD Standalone (Autonome) pour le FDM

Vous pouvez utiliser le Gestionnaire de périphériques de pare-feu avec une instance native. Les instances de conteneur ne sont pas prises en charge. Les périphériques logiques autonomes fonctionnent seuls ou dans une paire haute accessibilité.

Avant de commencer

- Téléchargez l'image de l'application que vous souhaitez utiliser pour le périphérique logique à partir de Cisco.com), puis cette image sur Châssis Firepower 4100/9300 .
- 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
- Vous devez également configurer au moins une interface de données.
- 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
  - l'adresse IP du serveur DNS
  - Nom d'hôte et le nom de domaine Firewall Threat Defense

Procédure

Consultez le guide de configuration de Gestionnaire de périphériques de pare-feu pour commencer à configurer votre politique de sécurité.

Ajouter une paire à haute disponibilité

La haute disponibilité Firewall Threat Defense (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 requise pour la haute accessibilité, à la page 212.

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 Haute disponibilité (basculement), à la page 203.

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.

Modifier une interface sur un périphérique logique FTD

Vous pouvez allouer ou annuler l'allocation d'une interface sur le périphérique logique Firepower Threat Defense. Vous pouvez ensuite synchroniser la configuration de l'interface dans FDM.

L'ajout d'une nouvelle interface ou la suppression d'une interface inutilisée a une incidence minime sur la configuration Firepower Threat Defense. Cependant, la suppression d'une interface utilisée dans votre politique de sécurité aura une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration Firepower Threat Defense, notamment les règles d'accès, la NAT, le SSL, les règles d'identité, le VPN, le serveur DHCP, etc. Les politiques qui font référence aux zones de sécurité ne sont pas touchées. Vous pouvez également modifier les membres d'un EtherChannel alloué sans affecter le périphérique logique ou nécessiter de synchronisation sur sur FDM.

vous pouvez migrer la configuration d'une interface à une autre avant de supprimer l'ancienne interface.

Avant de commencer

- Configurez vos interfaces et ajoutez tous les EtherChannels en fonction de Configurer une interface physique, à la page 195 et Ajouter un canal EtherChannel (canal de port), à la page 196.
- 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.
- Pour la mise en la haute disponibilité, assurez-vous d'ajouter ou de supprimer l'interface sur toutes les unités avant de synchroniser la configuration dans FDM. Nous vous recommandons d'effectuer les modifications d'interface sur l'unité de , puis sur l'unité de . Notez que les nouvelles interfaces sont

ajoutées dans un état administrativement inactif, de sorte qu'elles n'affectent pas la surveillance des interfaces.

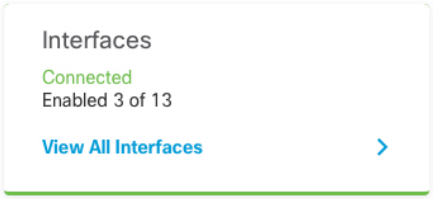
- En mode multi-instance, pour modifier une sous-interface par une autre sous-interface avec la même balise VLAN, vous devez d'abord supprimer toute la configuration (y compris la configuration Nameif) de l'interface, puis annuler l'allocation de l'interface dans Firepower Chassis Manager. Une fois non allouée, ajoutez la nouvelle interface, puis utilisez les interfaces de synchronisation de FMC.

Procédure

Étape 1 Synchroniser et migrer les interfaces dans le FDM.

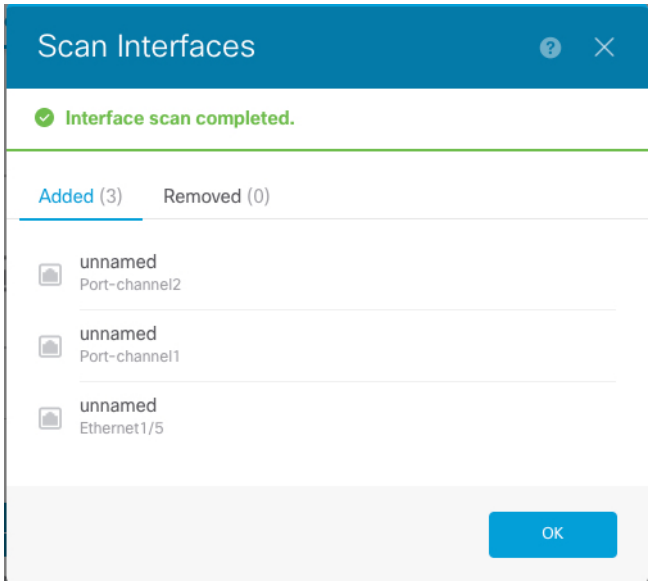
a) Connectez-vous à FDM.

b) Cliquez sur **Device** (Périphériques), puis sur le lien **View All Interfaces** (Afficher toutes les interfaces) du résume **Interfaces**.



c) Cliquez sur l'icône **Analyser les interfaces**.

d) Attendez que les interfaces effectuent l'analyse, puis cliquez sur **OK**.



e) Configurez les nouvelles interfaces avec les noms, les adresses IP, etc.

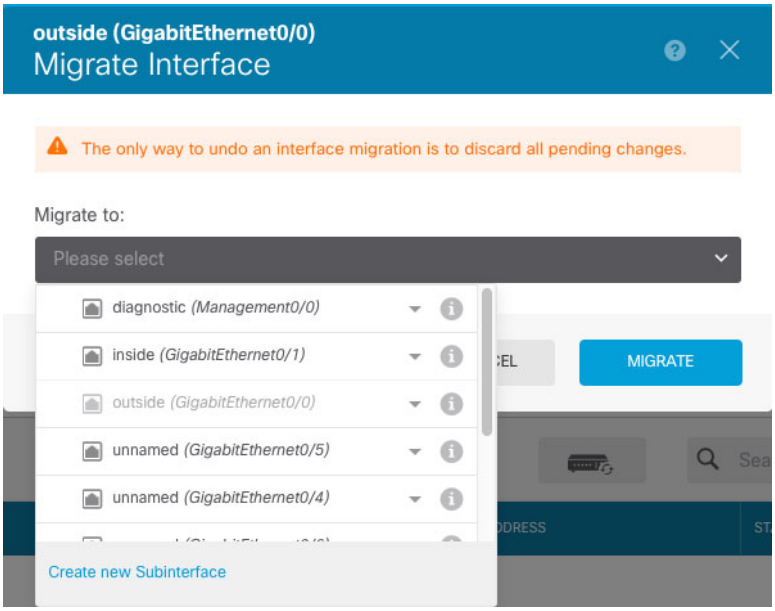
Si vous souhaitez utiliser l'adresse IP existante et le nom d'une interface que vous souhaitez supprimer, vous devez reconfigurer l'ancienne interface avec un nom et une adresse IP fictifs afin de pouvoir utiliser ces paramètres sur la nouvelle interface.

f) Pour remplacer une ancienne interface par une nouvelle interface, cliquez sur l'icône Remplacer par l'ancienne interface.

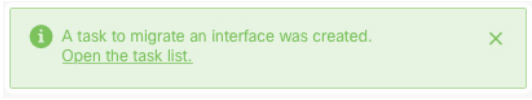
Icône Remplacer

Ce processus remplace l'ancienne interface par la nouvelle interface dans tous les paramètres de configuration qui font référence à l'interface.

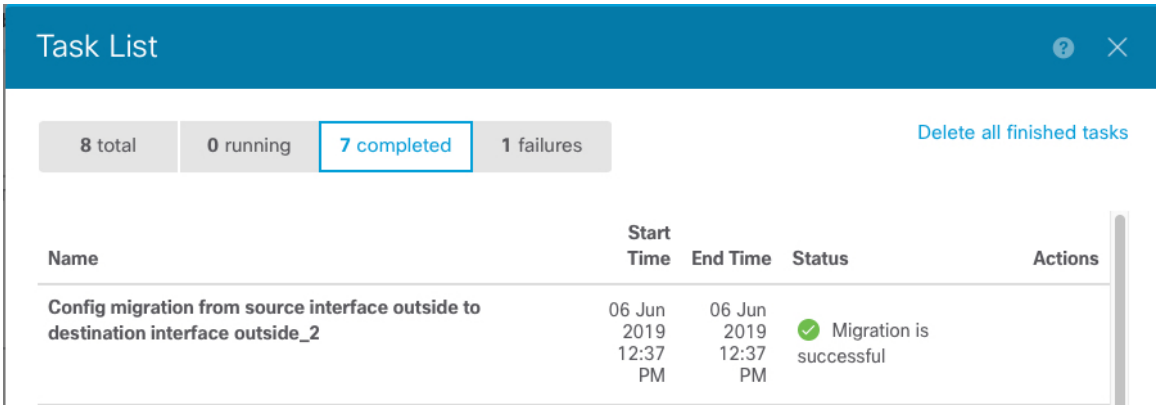
g) Choisissez la nouvelle interface dans la liste déroulante **Interface de remplacement**.



h) Un message s'affiche sur la page **Interfaces**. Cliquez sur le lien dans le message.

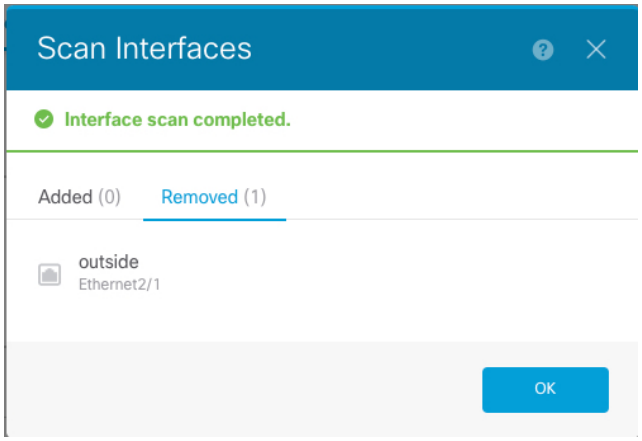


i) Vérifiez la **liste des tâches** pour vous assurer que la migration a réussi.



Étape 2 Synchronisez de nouveau les interfaces dans dans FDM.

Illustration 1 : Analyser les interfaces Gestionnaire de périphériques de pare-feu



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 ftd *name*

Pour afficher les noms des instances, entrez la commande sans nom.

Exemple :

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

Étape 3 Quittez la console d'application pour accéder à l'interface de ligne de commande du module FXOS.

- Firewall Threat Defense : Saisissez **exit**

Étape 4 Revenez au niveau de superviseur du 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-], .**

Historique des dispositifs logiques Firepower 4100/9300

Fonctionnalités	Version	Détails
Prise en charge de FDM sur le Firepower 4100/9300	6.5.0	Vous pouvez maintenant utiliser les dispositifs logiques FDM avec Firepower Threat Defense sur Firepower 4100/9300. Le FDM ne prend pas en charge la capacité multi-instance ; seules les instances natives sont prises en charge. **Remarque** Nécessite FXOS 2.7.1.



CHAPITRE 10

Haute disponibilité (basculement)

Les rubriques suivantes décrivent comment configurer et gérer le basculement actif/de secours pour atteindre la haute disponibilité du système Firewall Threat Defense.

- À propos de la haute disponibilité (basculement), à la page 203
- Configuration requise pour la haute accessibilité, à la page 212
- Lignes directrices pour la haute disponibilité, à la page 214
- Configuration de la haute disponibilité, à la page 215
- Gérer la haute disponibilité, à la page 229
- Surveillance de la haute disponibilité, à la page 241
- Dépannage de la haute disponibilité (basculement), à la page 244

À propos de la haute disponibilité (basculement)

Une configuration à haute disponibilité ou de basculement joint deux périphériques de sorte que si le périphérique principal tombe en panne, le périphérique secondaire peut prendre le relais. Cela vous aide à garder votre réseau opérationnel en cas de défaillance d'un périphérique.

La configuration de la haute disponibilité nécessite deux périphériques Firepower Threat Defense identiques connectés l'un à l'autre par un lien de basculement dédié et, éventuellement, un lien d'état. Les deux unités communiquent en permanence sur le lien de basculement pour déterminer l'état de fonctionnement de chacune d'elles et pour synchroniser les modifications de configuration déployées. Le système utilise le lien d'état pour transmettre les informations d'état de connexion au périphérique de secours, de sorte que si un basculement se produit, les connexions des utilisateurs sont conservées.

Les unités forment une paire active/en veille, où l'unité principale est l'unité active et transmet le trafic. L'unité secondaire (en veille) ne transmet pas activement le trafic, mais synchronise la configuration et les autres renseignements d'état de l'unité active.

L'intégrité de l'unité active (matériel, interfaces, logiciels et état environnemental) est surveillée pour déterminer si les conditions spécifiques au basculement sont respectées. Si ces conditions sont remplies, l'unité active bascule vers l'unité en veille, qui devient alors active.

À propos du basculement actif/de secours

Le basculement actif/en veille vous permet d'utiliser un Appareil FTD de secours pour reprendre les fonctionnalités d'une unité en panne. Lorsque l'unité active tombe en panne, l'unité en veille devient l'unité active.

Rôles principal/secondaire et état actif/de secours

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

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 secours.
- 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 secours.

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 secours, et toute remarque spéciale sur la condition et les actions de basculement.

Tableau 7 : 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	Politique	Action de l'unité active	Action de l'unité de secours	Notes
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.
Échec du 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.

Liens de basculement et de basculement avec état

Le lien de basculement est une connexion dédiée entre les deux unités. Le lien de basculement avec état est également une connexion dédiée, mais vous pouvez soit utiliser le lien de basculement comme lien de basculement/avec état combiné, soit créer un lien d'état dédié distinct. Si vous utilisez uniquement le lien de basculement, les informations sur l'état passent également par ce lien; vous ne perdez pas la capacité de basculement avec état.

Par défaut, les communications sur les liens de basculement et de basculement avec état sont en texte brut (non chiffré). Vous pouvez chiffrer les communications pour une sécurité renforcée en configurant une clé de chiffrement IPsec.

Les rubriques suivantes expliquent ces interfaces plus en détail et comprennent des recommandations sur la façon de câbler les périphériques pour obtenir les meilleurs résultats.

Lien 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 et synchroniser les modifications de configuration.

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
- Mises à jour des bases de données du système, y compris la VDB et les règles, mais excluant les bases de données de géolocalisation et de Security Intelligence. Chaque système télécharge séparément les mises à jour de géolocalisation et de Security Intelligence. Si vous créez un calendrier de mise à jour, ceux-ci doivent rester synchronisés. Toutefois, si vous effectuez une mise à jour manuelle de géolocalisation ou de Security Intelligence sur le périphérique actif, vous devez également en faire une sur le périphérique en veille.



Remarque Les données d'événements, de rapports et du journal d'audit ne sont pas synchronisées. La visionneuse d'événements et les tableaux de bord affichent uniquement les données liées à l'unité concernée. En outre, l'historique de déploiement, l'historique des tâches et les autres événements du journal d'audit ne sont pas synchronisés.

Lien de basculement dynamique

Le système utilise la liaison d'état pour transmettre les informations d'état de connexion au périphérique de secours. Ces informations aident l'unité de secours à maintenir les connexions existantes en cas de basculement.

L'utilisation d'une liaison unique pour les liens de basculement et de basculement dynamique est la meilleure façon de conserver les interfaces. Cependant, vous devez envisager une interface dédiée pour le lien d'état et le lien de basculement, si votre configuration est importante et que le trafic sur le réseau est élevé.

Interfaces pour les liens de basculement et d'état

Vous pouvez utiliser une interface de données inutilisée, mais activée (physique 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). Vous ne pouvez pas utiliser une interface de gestion, sous-interface, une interface VLAN ou un port de commutation pour le basculement.

L'appareil Firepower Threat Defense ne prend pas en charge le partage des interfaces entre les données utilisateur et le lien de basculement.

Consultez les consignes suivantes concernant la taille de la liaison de basculement et de l'état :

- Firepower 4100/9300 : nous vous recommandons d'utiliser une interface de données de 10 Go pour la combinaison de liaison de basculement et de liaison d'état.

- Tous les autres modèles : l'interface de 1 Go est suffisante pour une combinaison de liaison de basculement et d'état.

Lorsque vous utilisez une interface EtherChannel comme liaison de basculement ou d'état, vous devez confirmer que la même interface EtherChannel avec le même ID et les mêmes interfaces membres existe sur les deux appareils avant d'établir la haute disponibilité. S'il y a une incompatibilité EtherChannel, vous devez désactiver la HA, puis corriger la configuration sur l'unité secondaire avant de poursuivre. 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 des interfaces de basculement et de basculement dynamique

Vous pouvez utiliser toutes les interfaces physiques de données inutilisées comme liaison de basculement et liaison d'état dédiée facultative. Cependant, vous ne pouvez pas sélectionner une interface actuellement configurée avec un nom ou une interface qui comporte des sous-interfaces. Les interfaces de liaison de basculement et de basculement avec état ne sont pas configurées comme des interfaces réseau normales; elles existent uniquement pour la communication de basculement. Ils existent uniquement pour les communications de basculement, et vous ne pouvez pas les utiliser pour le trafic de transit ou l'accès de gestion.

Comme la configuration est synchronisée entre les périphériques, vous devez sélectionner le même numéro de port pour chaque extrémité de liaison. Par exemple, GigabitEthernet1/3 sur les deux appareils pour le lien de basculement.

Connectez le lien de basculement, et le lien d'état dédié si utilisé, 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 du périphérique Firepower Threat Defense. Une liaison d'état dédiée a les mêmes exigences, mais doit se trouver sur un segment de réseau différent de celui de la liaison de basculement.



Remarque L'intérêt de l'utilisation d'un commutateur est que si l'une des interfaces de l'unité tombe en panne, il est facile de déterminer quelle interface est défaillante. Si vous utilisez une connexion directe par câble, en cas de défaillance d'une interface, la liaison est interrompue sur les deux homologues, ce qui rend difficile de déterminer quel périphérique est défectueux.

- L'utilisation d'un câble Ethernet pour connecter les unités directement, sans avoir besoin d'un commutateur externe. Le périphérique Firepower Threat Defense prend en charge Auto-MDI/MDIX sur ses ports Ethernet en cuivre ; vous pouvez donc utiliser un câble croisé ou un câble droit. Si vous utilisez un câble droit, l'interface détecte automatiquement le câble et échange l'une des paires de transmission/réception contre MDIX.

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 le lien de basculement est arrêté, l'appareil Firepower Threat Defense 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 du lien 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 périphériques Firepower Threat Defense, quand un commutateur ou une liaison inter-commutateurs sont en panne, les deux périphériques deviennent actifs.Firepower Threat Defense Par conséquent, les deux méthodes de connexion indiquées dans les figures suivantes ne sont **pas** recommandées.

Illustration 2 : Connexion avec un commutateur unique : non recommandée

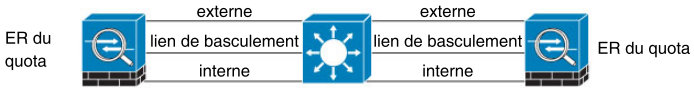
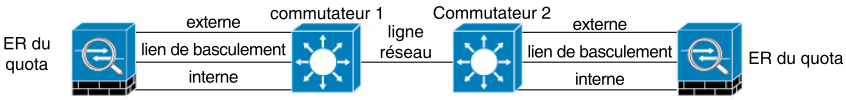


Illustration 3 : Connexion avec un double commutateur : non recommandée



Scénario 2 (recommandé)

Nous recommandons que les liens 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 le lien de basculement, comme le montrent les figures suivantes.

Illustration 4 : Connexion avec un autre commutateur

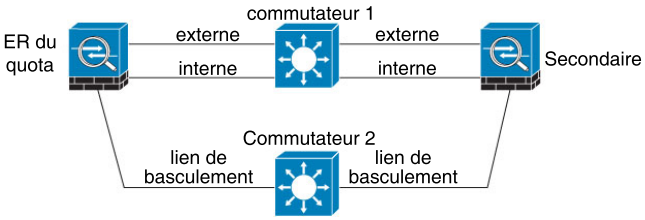
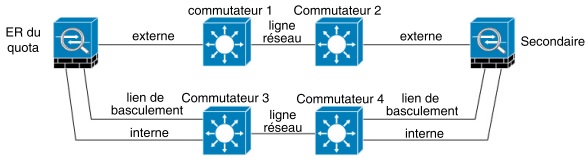


Illustration 5 : Connexion avec un câble

Scénario 3 (recommandé)

Si les interfaces de données Firepower Threat Defense sont connectées à plusieurs ensembles de commutateurs, un lien 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 6 : Connexion avec un commutateur sécurisé



Incidence du basculement dynamique sur les connexions utilisateur

L'unité active partage les informations sur l'état de la connexion avec l'unité de secours. Cela signifie que l'unité de secours peut maintenir certains types de connexions sans nuire à l'utilisateur.

Cependant, il existe certains types de connexions qui ne prennent pas en charge le basculement avec état. Pour ces connexions, l'utilisateur devra rétablir la connexion en cas de basculement. Souvent, cela se produit automatiquement en fonction du comportement du protocole utilisé dans la connexion.

Les rubriques suivantes expliquent quelles fonctionnalités sont prises en charge ou non pour le basculement avec état.

Fonctionnalités prises en charge

Pour le basculement avec état, les renseignements d'état suivants sont transmis à l' Appareil FTD de secours :

- table de traduction NAT
- Les connexions et les états TCP et UDP, y compris les états des connexions HTTP. 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.
- États de connexion Snort, résultats d'inspection et informations sur les trous d'épingle, y compris une application stricte du protocole TCP.
- 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.
- 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.
- Décisions relatives à la politique de contrôle d'accès : les décisions relatives à la correspondance du trafic (y compris l'URL, la catégorie d'URL, la géolocalisation, etc.), la détection des intrusions, les programmes malveillants et le type de fichier sont conservées pendant le basculement. Cependant, pour les connexions évaluées au moment du basculement, les mises en garde suivantes doivent être apportées :
  - AVC : Les verdicts d'ID d'application sont répliqués, mais pas les états de détection. Une synchronisation appropriée a lieu tant que les verdicts App-ID sont complets et synchronisés avant le basculement.
  - État de la détection d'intrusion : lors du basculement, une fois que le prélèvement en milieu de flux se produit, de nouvelles inspections sont effectuées, mais les anciens états sont perdus.
  - Blocage des programmes malveillants : l'élimination des fichiers doit être disponible avant le basculement.
  - Détection et blocage du type de fichier : le type de fichier doit être identifié avant le basculement. Si le basculement se produit pendant que le périphérique actif d'origine identifie le fichier, le type de fichier n'est pas synchronisé. Même si votre politique de fichiers bloque ce type de fichier, le nouveau périphérique actif télécharge le fichier.
- Décisions relatives à l'identité de l'utilisateur passif de la politique d'identité, mais pas celles recueillies lors de l'authentification active sur un portail captif.
- Décisions en matière de renseignements sur la sécurité.
- 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

Pour le basculement avec état, les informations d'état suivantes ne sont pas transmises au Appareil FTD de secours :

- Sessions dans des tunnels en texte brut comme GRE ou IP-in-IP. Les sessions à l'intérieur des tunnels ne sont pas répliquées et le nouveau nœud actif ne pourra pas réutiliser les verdicts d'inspection existants pour faire correspondre les règles de politique correctes.
- Connexions TLS/SSL déchiffrées : les états de déchiffrement ne sont pas synchronisés et si l'unité active échoue, les connexions déchiffrées seront réinitialisées. De nouvelles connexions devront être établies avec la nouvelle unité active. Les connexions qui ne sont pas déchiffrées (c'est-à-dire celles qui correspondent à une action de règle Ne pas déchiffrer de TLS/SSL) ne sont pas affectées et sont répliquées correctement.
- Le routage de multidiffusion

Modifications de configuration et actions autorisées sur une unité de secours

Lorsque vous fonctionnez en mode de haute disponibilité, vous apportez des modifications de configuration à l'unité active uniquement. Lorsque vous déployez la configuration, les nouvelles modifications sont également transmises à l'unité de secours.

Cependant, certaines propriétés sont uniques à l'unité de secours. Vous pouvez modifier les éléments suivants sur une unité de secours :

- Adresse IP de l'interface de gestion et passerelle.
- (Interface de ligne de commande uniquement.) Le mot de passe du compte d'utilisateur admin et des autres comptes d'utilisateurs locaux. Vous pouvez effectuer cette modification dans l'interface de ligne de commande uniquement ; vous ne pouvez pas la faire dans Gestionnaire de périphériques de pare-feu. Tout utilisateur local devra modifier son mot de passe sur les deux unités séparément.

En outre, les actions suivantes sont disponibles sur un périphérique de secours.

- Actions de haute disponibilité, telles que la suspension, la reprise, la réinitialisation et l'interruption de la haute disponibilité, ainsi que la commutation des modes entre actif et en veille.
- Les données de tableau de bord et d'événements sont propres à chaque périphérique et ne sont pas synchronisées. Cela inclut les affichages personnalisés dans Event Viewer (Visionneuse d'événements)
- Les informations du journal d'audit sont uniques par périphérique.
- Enregistrement de licence Smart. Cependant, vous devez activer ou désactiver les licences facultatives sur l'unité active, et l'action est synchronisée avec l'unité de secours, qui demande ou libère la licence appropriée.
- Sauvegarde, mais pas restauration. Vous devez interrompre la haute disponibilité sur l'unité pour restaurer une sauvegarde. Si la sauvegarde comprend la configuration à haute disponibilité, l'unité rejoindra le groupe à haute disponibilité.
- Installation de mise à niveau logicielle.
- Génération de journaux de dépannage.
- Mise à jour manuelle des bases de données de géolocalisation ou de Security Intelligence. Ces bases de données ne sont pas synchronisées entre les unités. Si vous créez un calendrier de mise à jour, les unités peuvent maintenir indépendamment la cohérence.
- Vous pouvez afficher les sessions utilisateur Gestionnaire de périphériques de pare-feu actives et supprimer des sessions à partir de la page **Monitoring** > **Sessions** > **(sessions de surveillance)** .

Configuration requise pour la haute accessibilité

Les rubriques suivantes expliquent les exigences à respecter avant d'intégrer deux périphériques dans une configuration à haute accessibilité.

Configuration matérielle requise pour la haute disponibilité

Pour relier deux appareils dans une configuration à haute disponibilité, vous devez satisfaire aux exigences matérielles suivantes.

- Les appareils doivent être du même modèle exactement.

  Pour la Firepower 9300, la haute disponibilité est uniquement prise en charge entre les modules de même type; toutefois, les deux châssis peuvent inclure des modules mixtes. Par exemple, chaque châssis comporte un SM-36 et un SM-44. Vous pouvez créer des paires haute disponibilité entre les modules SM-36 et entre les modules SM-44.

- Les appareils doivent avoir le même nombre et le même type d'interfaces.

  Pour le châssis Firepower 4100/9300, toutes les interfaces doivent être préconfigurées de manière identique dans FXOS avant que vous activiez la haute disponibilité. 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.

- Les mêmes modules doivent être installés sur les appareils. Par exemple, si l'un comporte un module d'interface réseau facultatif, vous devez installer le même module dans l'autre périphérique.

- La haute disponibilité intra-châssis pour Firepower 9300 n'est pas prise en charge. Vous ne pouvez pas configurer la haute disponibilité entre des périphériques logiques distincts sur le même châssis Firepower 9300.

Configuration logicielle requise pour la haute disponibilité

Pour relier deux appareils dans une configuration à haute disponibilité, vous devez satisfaire aux exigences logicielles suivantes.

- Les appareils doivent présenter exactement la même version de logiciel, ce qui signifie les mêmes numéros majeur (premier), mineur (deuxième) et de maintenance (troisième). Vous pouvez trouver la version dans le Gestionnaire de périphériques de pare-feu sur la page **Devices (appareils)**, ou vous pouvez utiliser la commande **show version** dans l'interface de ligne de commande. Les appareils de versions différentes sont autorisés à s'associer, mais la configuration n'est pas importée dans l'unité en veille et le basculement ne fonctionne pas tant que vous ne mettez pas les unités à niveau vers la même version logicielle.

- Les deux appareils doivent être en mode gestionnaire local, c'est-à-dire configurés à l'aide de la fonction Gestionnaire de périphériques de pare-feu. Si vous pouvez vous connecter au Gestionnaire de périphériques de pare-feu sur les deux systèmes, ils sont en mode gestionnaire local. Vous pouvez également utiliser la commande **show managers** dans l'interface de ligne de commande pour vérifier.

- Vous devez exécuter l'assistant de configuration initiale pour chaque périphérique.

- Chaque périphérique doit avoir sa propre adresse IP de gestion. La configuration de l'interface de gestion n'est pas synchronisée entre les appareils.

- Les périphériques doivent avoir la même configuration NTP.
- Vous ne pouvez configurer aucune interface pour obtenir son adresse en utilisant DHCP. Autrement dit, toutes les interfaces doivent avoir des adresses IP statiques.
- Pour les services en nuage, les deux appareils doivent être enregistrés dans la même région ou aucun appareil ne peut être inscrit. Vous ne pouvez pas avoir des enregistrements mixtes aux services en nuage.
- Vous devez déployer toutes les modifications en attente avant de configurer la haute disponibilité.

Exigences en matière de licence pour la haute disponibilité

Avant de configurer la haute disponibilité, les unités doivent être dans le même état : soit les deux sont enregistrées avec une licence De base, soit les deux sont enregistrées dans un mode d'évaluation. Si les périphériques sont enregistrés, ils peuvent être enregistrés dans différents comptes Cisco Smart Software Manager, mais les comptes doivent avoir le même état pour le paramètre de fonctionnalité de contrôle de l'exportation : activés ou désactivés. Cependant, il importe peu que vous ayez activé ou non différentes licences facultatives sur les unités. Si vous enregistrez les deux unités, vous devez sélectionner la même région Cisco Cloud Services pour les appareils.

Si les appareils sont enregistrés, ils doivent utiliser le même mode, soit Smart License ou Permanent License Reservation (PLR).

Pendant le fonctionnement, les unités de la paire à haute disponibilité doivent avoir les mêmes licences. Toutes les modifications de licence que vous apportez à l'unité active sont répétées sur l'unité en veille pendant le déploiement.

Les configurations à haute disponibilité nécessitent deux licences Smart; une pour chaque appareil de la paire. Vous devez vous assurer que les licences dans votre compte sont en nombre adéquat pour s'appliquer à chaque appareil. Il est possible d'être en conformité sur un appareil, mais non sur l'autre, si le nombre de licences est insuffisant.

Par exemple, si le périphérique actif possède la licence De base et que le Menace , et le périphérique en veille ne possède que la licence De base, l'unité en veille communique avec Cisco Smart Software Manager pour obtenir un Menace disponible à partir de votre compte. Si votre compte de licences Smart ne comprend pas suffisamment de droits achetés, votre compte devient non conforme (et l'appareil en veille est non conforme même si l'appareil actif est conforme) jusqu'à ce que vous achetiez le nombre correct de licences.

À superviser :

- Si vous enregistrez les appareils dans des comptes qui ont des paramètres différents pour les fonctions contrôlées à l'exportation, ou essayez de créer une paire haute accessibilité avec une unité enregistrée et l'autre en mode d'évaluation, la jonction haute accessibilité peut échouer.
- Si vous configurez une clé de chiffrement IPsec avec des paramètres incohérents pour les fonctionnalités contrôlées à l'exportation, les deux appareils deviendront actifs après l'activation de la haute accessibilité. Cela aura une incidence sur le routage des segments de réseau pris en charge, et vous devrez interrompre manuellement la haute accessibilité sur l'unité secondaire pour récupérer.
- Ne modifiez pas les licences au milieu de la création du groupe à haute disponibilité. Les deux unités doivent avoir la même configuration au moment de la jonction de la haute disponibilité, sinon vous verrez l'erreur suivante : « Échec de la validation FDM – Incompatibilité de l'état d'inscription du service en nuage entre le nœud principal et le nœud secondaire. Consultez l'interface CLI app-sync-history pour en savoir plus. »

Lignes directrices pour la haute disponibilité

Prise en charge des modèles

- Firepower 9300 : vous pouvez configurer la haute disponibilité sur le Firepower 9300. Cependant, vous ne pouvez pas configurer la haute disponibilité entre des dispositifs logiques distincts sur le même châssisFirepower 9300.
- Firepower 1010 :
  - Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l'utilisation de Haute disponibilité. 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. Haute disponibilité 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 Haute disponibilité 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 Haute disponibilité 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.
  - Lorsque le châssis est dans une paire à haute accessibilité, le voyant DEL de l'unité en veille est ambre.
- (Série Firepower 1000, Firepower 2100)—Le déploiement de périphériques en haute disponibilité avec des centaines d'interfaces configurées peut entraîner une augmentation du délai de basculement (en secondes).
- FTDv : la configuration à haute disponibilité n'est pas prise en charge pour FTDv pour le nuage Microsoft Azure ou le nuage Amazon Web Services (AWS).

Directives supplémentaires

- 169.254.0.0/16 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne et ne peuvent pas être utilisés pour le basculement ou les liens d'état.
- La configuration de l'unité active est synchronisée avec l'unité de secours lorsque vous exécutez une tâche de déploiement sur l'unité active. Cependant, certaines modifications ne s'affichent pas dans les modifications en attente, même si elles ne sont pas synchronisées sur l'unité de secours jusqu'à ce que vous déployiez les modifications. Si vous modifiez l'un des éléments suivants, les modifications sont masquées et vous devez exécuter une tâche de déploiement avant qu'elles ne soient configurées sur l'unité de secours. Si vous devez appliquer la modification immédiatement, vous devrez apporter une autre modification qui ne s'affiche pas dans les modifications en attente. Les modifications masquées comprennent la modification des éléments suivants : les planifications des mises à jour des règles, de la base de données de géolocalisation, des renseignements de sécuritéou de la VDB ; les planifications des sauvegardes ; NTP ; DNS pour l'interface de gestion ; Serveur mandataire HTTP pour les connexions de gestion ; droits de licence ; options des services en nuage ; options de filtrage d'URL.

- Vous devez effectuer des sauvegardes sur les unités principale et secondaire. Pour restaurer une sauvegarde, vous devez d'abord interrompre la haute disponibilité. Ne restaurez pas la même sauvegarde sur les deux unités, car elles deviendraient alors actives. Au lieu de cela, restaurez la sauvegarde sur l'unité que vous souhaitez rendre active en premier, puis restaurez la sauvegarde équivalente sur l'autre unité.
- Le bouton **Test** (Tester) pour les différentes sources d'identité fonctionne uniquement sur l'unité active. Si vous devez tester la connectivité de la source d'identité pour le périphérique en veille, vous devez d'abord changer de mode pour faire de l'homologue en veille l'homologue actif.
- La création ou l'interruption de la configuration à haute disponibilité redémarre le processus d'inspection Snort sur les deux périphériques lorsque la modification de configuration est déployée. Cela peut entraîner une perturbation du trafic jusqu'à ce que le processus soit complètement redémarré.
- Lors de la configuration initiale de la haute disponibilité, si les versions des bases de données de renseignements de sécurité et de géolocalisation sur l'unité secondaire sont différentes de celles de l'unité principale, les tâches de mise à jour des bases de données sont planifiées sur l'unité secondaire. Ces tâches sont exécutées lors du prochain déploiement à partir de l'unité active. Même si la jonction à haute disponibilité échoue, ces tâches demeurent et seront exécutées lors du prochain déploiement.
- 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 en haute disponibilité 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.
- En haute disponibilité active/en veille avec un tunnel VPN IPsec, vous ne pouvez pas superviser à la fois l'unité active et l'unité de secours au moyen de SNMP via le tunnel VPN. L'unité de secours n'a pas de tunnel VPN actif et laissera tomber le trafic destiné au système de gestion de réseau (NMS). Vous pouvez plutôt utiliser SNMPv3 avec chiffrement pour que le tunnel IPsec ne soit pas requis.
- Les interfaces que vous utilisez pour les liens de basculement à haute disponibilité et de basculement dynamique ne doivent pas être activées. L'état de l'interface devrait indiquer que la liaison est activée, mais les interfaces elles-mêmes peuvent sembler désactivées. En outre, les informations d'interface ne sont pas mises à jour avec les adresses IP définies dans la configuration de haute disponibilité.

Configuration de la haute disponibilité

Utilisez une configuration à haute disponibilité pour assurer la connectivité réseau même en cas de défaillance d'un périphérique. Avec la haute disponibilité active/en veille, deux périphériques sont liés, de sorte que, si le périphérique actif tombe en panne, le périphérique en veille prend le relais et les utilisateurs ne devraient voir qu'un bref problème de connectivité.

La procédure suivante explique le processus de bout en bout pour configurer une paire de haute disponibilité (HA) active/en veille.

Procédure

Étape 1 Préparer les deux unités pour la haute disponibilité, à la page 216.

Étape 2 Configurer l'unité principale pour la haute disponibilité, à la page 218.

Étape 3 Configurer l'unité secondaire pour la haute disponibilité, à la page 221.

Étape 4 Configurer les critères de basculement pour la surveillance de l'intégrité, à la page 222.

Les critères comprennent la surveillance des homologues et la surveillance des interfaces. Bien que tous les critères de basculement aient des paramètres par défaut, vous devez au moins les examiner pour vérifier que les paramètres par défaut fonctionnent pour votre réseau.

- Configurer les critères de basculement de la surveillance de l'intégrité des unités homologues, à la page 223.
- Configurer les critères de basculement pour la surveillance de l'intégrité des interfaces, à la page 224.

  Pour en savoir plus sur les tests d'interface, consultez Comment le système teste l'intégrité de l'interface, à la page 226.

Étape 5 (Facultatif, mais conseillé.) Configurer les adresses IP et MAC de secours, à la page 227.

Étape 6 (Facultatif) Vérifier la High Availability Configuration (Configuration de la haute disponibilité) , à la page 228.

Préparer les deux unités pour la haute disponibilité

Il y a beaucoup de choses que vous devez préparer correctement avant de pouvoir configurer la haute disponibilité.

Procédure

Étape 1 Assurez-vous que les appareils répondent aux exigences décrites dans Configuration matérielle requise pour la haute disponibilité, à la page 212.

Étape 2 Déterminez si vous allez utiliser un seul lien de basculement ou des liens distincts de basculement et de basculement avec état, puis définissez les ports que vous utiliserez.

Vous devez utiliser le même numéro de port sur chaque périphérique pour chaque lien. Par exemple, GigabitEthernet 1/3 sur les deux appareils pour le lien de basculement. Sachez lesquels vous utiliserez afin de ne pas les utiliser accidentellement à d'autres fins. Pour en savoir plus, consultez Liens de basculement et de basculement avec état, à la page 205.

Étape 3 Installez les périphériques, connectez-les au réseau et exécutez l'assistant de configuration initiale sur chaque périphérique.

a) Passez en revue les conceptions de réseau recommandées dans Éviter le basculement interrompu et les liaisons de données, à la page 208.

b) Connectez au moins les interfaces externes, comme expliqué dans Connecter les interfaces, à la page 21.

Vous pouvez également connecter les autres interfaces, mais vous devez vous assurer d'utiliser le même port sur chaque périphérique pour vous connecter à un sous-réseau donné. Comme les appareils partagent la même configuration, vous devez les connecter à vos réseaux en parallèle.

Remarque
L'assistant de configuration ne vous permet pas de modifier les adresses IP sur l'interface de gestion et l'interface interne. Ainsi, si vous connectez l'une de ces interfaces sur le périphérique principal avec le réseau, ne connectez pas non plus les interfaces sur le périphérique secondaire, sinon vous aurez un conflit d'adresses IP. Vous pouvez connecter directement votre poste de travail à l'une de ces interfaces et obtenir une adresse au moyen du protocole DHCP, afin de pouvoir vous connecter à Gestionnaire de périphériques de pare-feu et configurer l'appareil.

c) Terminez l'assistant de configuration initiale sur chaque périphérique. Assurez-vous de spécifier des adresses IP statiques pour l'interface externe. En outre, configurez les mêmes serveurs NTP. Pour en savoir plus, consultez Compléter la configuration initiale avec l'assistant d'installation, à la page 23.

Choisissez les mêmes licences et options de Cisco Success Network (Réseau de succès Cisco) pour les unités. Par exemple, le mode d'évaluation pour chacun ou l'enregistrement des appareils.

d) Sur le périphérique secondaire, sélectionnez **Device (périphérique)** > **System Settings (paramètres système)** > **Management Interface (interface de gestion)** et configurez une adresse IP unique, modifiez la passerelle si nécessaire, puis désactivez ou modifiez les paramètres du serveur DHCP selon vos besoins.
e) Sur le périphérique secondaire, sélectionnez l'interface de périphérique **Device** > **Interface** et modifiez l'interface interne. Supprimez l'adresse IP ou modifiez-la. Supprimez également le serveur DHCP défini pour l'interface, car vous ne pouvez pas avoir deux serveurs DHCP sur le même réseau.
f) Déployez la configuration sur le périphérique secondaire.
g) Si nécessaire, en fonction de votre topologie de réseau, connectez-vous au périphérique principal et modifiez l'adresse de gestion, la passerelle et les paramètres du serveur DHCP, ainsi que l'adresse IP de l'interface interne et les paramètres du serveur DHCP. Déployez la configuration si vous apportez des modifications.
h) Si vous n'avez pas connecté l'interface interne ou l'interface de gestion si vous utilisez un réseau de gestion distinct, vous pouvez maintenant les connecter aux commutateurs.

Étape 4 Vérifiez que les appareils présentent exactement la même version de logiciel, ce qui signifie les mêmes numéros majeur (premier), mineur (deuxième) et de maintenance (troisième). Vous pouvez trouver la version dans le Gestionnaire de périphériques de pare-feu sur la page Devices (appareils), ou vous pouvez utiliser la commande **show version** dans l'interface de ligne de commande.

S'ils n'exécutent pas les mêmes versions de logiciel, procurez-vous la version de logiciel préférée sur Cisco.com et installez-la sur chaque appareil. Pour de plus amples renseignements, consultez la section Mise à niveau Firewall Threat Defense, à la page 824.

Étape 5 Connectez et configurez les liens de basculement et de basculement avec état.

a) Selon votre conception de réseau préférée (choisie depuis Éviter le basculement interrompu et les liaisons de données, à la page 208), connectez les interfaces de basculement de chaque périphérique de manière appropriée, soit avec un commutateur, soit directement les unes avec les autres.
b) Si vous utilisez un lien d'état distinct, connectez également les interfaces de basculement avec état pour chaque périphérique de manière appropriée.
c) Connectez-vous à chaque appareil à son tour et accédez à l'interface de périphérique (**Device** > **Interface**). Modifiez chaque interface et vérifiez qu'il n'y a pas de noms d'interface ou d'adresses IP configurés.

Si les interfaces sont configurées avec des noms, vous devrez peut-être les supprimer des zones de sécurité et supprimer d'autres configurations avant de pouvoir supprimer le nom. Si la suppression du nom échoue, examinez les messages d'erreur pour déterminer les autres modifications à apporter.

Étape 6 Sur le périphérique principal, connectez les interfaces de données restantes et configurez le périphérique.

a) Sélectionnez **Device** > **Interface** (interface de périphérique), modifiez chaque interface utilisée pour le trafic traversant et configurez les adresses IP statiques principales.

b) Ajoutez les interfaces aux zones de sécurité et configurez les politiques de base nécessaires pour gérer le trafic sur les réseaux connectés. Pour des exemples de configurations, consultez la liste des rubriques dans Meilleures pratiques : scénarios d'utilisation pour Firewall Threat Defense, à la page 43.

c) Déployez la configuration.

Étape 7 Vérifiez que vous répondez à toutes les exigences décrites dans Configuration logicielle requise pour la haute disponibilité, à la page 212.

Étape 8 Vérifiez que les licences sont cohérentes (enregistrement des appareils ou mode d'évaluation). Pour en savoir plus, consultez Exigences en matière de licence pour la haute disponibilité, à la page 213.

Étape 9 Sur le périphérique secondaire, connectez les interfaces de données restantes aux mêmes réseaux que les interfaces équivalentes sur le périphérique principal. Ne configurez pas les interfaces.

Étape 10 Sur chaque appareil, sélectionnez **Périphérique** > **Paramètres du système** > **Services en nuage** et vérifiez que vous avez les mêmes paramètres.

Vous êtes maintenant prêt à configurer la haute disponibilité sur l'appareil principal.

Configurer l'unité principale pour la haute disponibilité

Pour configurer une paire à haute disponibilité actif/en veille, vous devez d'abord configurer le périphérique principal. L'appareil principal est l'unité qui doit être active dans des circonstances normales. L'appareil secondaire reste en mode veille jusqu'à ce que l'unité principale ne soit plus disponible.

Sélectionnez le périphérique que vous souhaitez être principal, puis connectez-vous au Gestionnaire de périphériques de pare-feu sur ce périphérique et suivez cette procédure.

Remarque Une fois la paire de haute disponibilité établie, vous devez rompre la paire afin de modifier la configuration décrite dans cette procédure.

Avant de commencer

Assurez-vous que les interfaces que vous configurerez pour le lien de basculement et le lien de basculement dynamique ne portent aucun nom. Si elles sont actuellement nommées, vous devez supprimer les interfaces de toutes les politiques qui les utilisent, y compris les objets de zone de sécurité, puis modifier les interfaces pour supprimer le nom. Les interfaces doivent également être en mode routé, et non en mode passif. Ces interfaces doivent être dédiées à une utilisation dans la configuration à haute disponibilité : vous ne pouvez pas les utiliser à d'autres fins.

Si des modifications sont en attente, vous devez les déployer avant de pouvoir configurer la haute disponibilité.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Dans la partie droite du résumé du périphérique, cliquez sur **Configure** (Configurer) à côté du groupe **High Availability** (Haute disponibilité).

Si vous configurez la haute disponibilité pour la première fois sur le périphérique, le groupe ressemblerait à ce qui suit.



Étape 3 Sur la page High Availability (Haute disponibilité), cliquez sur la case **Primary Device** (Périphérique principal).

Si le périphérique secondaire est déjà configuré et que vous avez copié la configuration dans le presse-papiers, vous pouvez cliquer sur le bouton **Paste from Clipboard** (Coller à partir du presse-papiers) et coller la configuration. Cela mettra à jour les champs avec les valeurs appropriées, que vous pourrez ensuite vérifier.

Étape 4 Configurez les propriétés du **Failover Link** (Lien 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 et synchroniser les modifications de configuration. Pour en savoir plus, consultez Lien de basculement, à la page 206.

- **Physical Interface** (Interface physique) : sélectionnez l'interface que vous avez connectée au périphérique secondaire pour l'utiliser comme lien de basculement. Il doit s'agir d'une interface sans nom.

  Lorsque vous utilisez une interface EtherChannel comme liaison de basculement ou d'état, vous devez confirmer que la même interface EtherChannel avec le même ID et les mêmes interfaces membres existe sur les deux appareils avant d'établir la haute disponibilité. S'il y a une incompatibilité EtherChannel, vous devez désactiver la HA, puis corriger la configuration sur l'unité secondaire avant de poursuivre. 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.

- **Type** : choisissez si vous utiliserez une adresse IPv4 ou IPv6 pour l'interface. Vous ne pouvez configurer qu'un seul type d'adresse.

- **Primary IP** (IP principale) : saisissez l'adresse IP de l'interface sur ce périphérique. Par exemple, 192.168.10.1. Pour les adresses IPv6, vous devez inclure la longueur du préfixe en notation standard, par exemple, 2001:a0a:b00::a0a:b70/64.

- **Secondary IP** (IP secondaire) : saisissez l'adresse IP à configurer à l'autre extrémité du lien, sur l'interface du périphérique secondaire. L'adresse doit se trouver sur le même sous-réseau que l'adresse principale et elle doit être différente de l'adresse principale. Par exemple, 192.168.10.2 ou 2001:a0a:b00::a0a:b71/64.

- **Netmask (IPv4 only)** (Masque réseau) (IPv4 uniquement) : saisissez le masque de sous-réseau pour l'adresse IP principale/secondaire.

Étape 5 Configurez les propriétés du Stateful Failover Link (Lien de basculement dynamique).

Le système utilise la liaison d'état pour transmettre les informations d'état de connexion au périphérique de secours. Ces informations aident l'unité de secours à maintenir les connexions existantes en cas de basculement. Vous pouvez soit utiliser la même liaison que la liaison de basculement, soit configurer une liaison distincte.

- **Use the Same Interface as the Failover Link** (Utiliser la même interface que le lien de basculement) : sélectionnez cette option si vous souhaitez utiliser un lien unique pour les communications de basculement et de basculement dynamique. Si vous sélectionnez cette option, passez à l'étape suivante.
- **Physical Interface** (Interface physique) : si vous souhaitez utiliser un lien de basculement dynamique distinct, sélectionnez l'interface que vous avez connectée au périphérique secondaire pour l'utiliser comme lien de basculement dynamique. Il doit s'agir d'une interface sans nom. Configurez les propriétés suivantes :
  - **Type** : choisissez si vous utiliserez une adresse IPv4 ou IPv6 pour l'interface. Vous ne pouvez configurer qu'un seul type d'adresse.
  - **Primary IP** (IP principale) : saisissez l'adresse IP de l'interface sur ce périphérique. L'adresse doit se trouver sur un sous-réseau différent de celui utilisé pour la liaison de basculement. Par exemple, 192.168.11.1. Pour les adresses IPv6, vous devez inclure la longueur du préfixe en notation standard, par exemple, 2001:a0a:b00:a::a0a:b70/64.
  - **Secondary IP** (IP secondaire) : saisissez l'adresse IP à configurer à l'autre extrémité du lien, sur l'interface du périphérique secondaire. L'adresse doit se trouver sur le même sous-réseau que l'adresse principale et elle doit être différente de l'adresse principale. Par exemple, 192.168.11.2 ou 2001:a0a:b00:a::a0a:b71/64.
  - **Netmask (IPv4 only)** (Masque réseau) (IPv4 uniquement) : saisissez le masque de sous-réseau pour l'adresse IP principale/secondaire.

Étape 6 (Facultatif) Saisissez une chaîne de **IPsec Encryption Key** (Clé de chiffrement IPsec) si vous souhaitez chiffrer les communications entre les deux unités de la paire.

Vous devez configurer exactement la même clé sur le nœud secondaire ; notez donc la chaîne que vous saisissez.

Si vous ne saisissez pas de clé, toutes les communications sur les liens de basculement et de basculement dynamique se font en texte brut. Si vous n'utilisez pas de connexions directes par câble entre les interfaces, il peut s'agir d'un problème de sécurité.

Remarque
Si vous configurez le chiffrement du basculement HA en mode d'évaluation, le système utilise DES comme algorithme de 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.

Étape 7 Cliquez sur **Activate HA** (Activer HA).

Le système déploie immédiatement la configuration sur le périphérique. Vous n'avez pas besoin de démarrer une tâche de déploiement. Si vous ne voyez pas de message indiquant que votre configuration a été enregistrée et que le déploiement est en cours, faites défiler la page vers le haut pour voir les messages d'erreur.

La configuration est également copiée dans le presse-papiers. Vous pouvez utiliser la copie pour configurer rapidement l'unité secondaire. Pour plus de sécurité, la clé de chiffrement n'est pas incluse dans la copie du presse-papiers.

Une fois la configuration terminée, vous recevez un message expliquant les prochaines étapes à suivre. Cliquez sur **Got It (J'ai compris)** après avoir pris connaissance des informations.

À ce stade, vous devriez vous trouver sur la page High Availability (Haute disponibilité), et l'état de votre périphérique devrait être Negotiating (Négociation). L'état doit passer à Active (Actif) même avant que vous ne configuriez l'unité homologue, laquelle doit apparaître comme Failed (En échec) jusqu'à sa configuration.



Vous pouvez maintenant configurer l'unité secondaire. Consultez Configurer l'unité secondaire pour la haute disponibilité, à la page 221.

Remarque
Les interfaces sélectionnées ne sont pas configurées directement. Toutefois, si vous saisissez **show interface** dans l'interface de ligne de commande, vous constaterez que les interfaces utilisent les adresses IP spécifiées. Les interfaces sont nommées « failover-link » et, si vous configurez une liaison d'état distincte, « stateful-failover-link ».

Configurer l'unité secondaire pour la haute disponibilité

Après avoir configuré le périphérique principal pour la haute disponibilité active/en veille, vous devez configurer le périphérique secondaire. Connectez-vous à Gestionnaire de périphériques de pare-feu sur ce périphérique et suivez cette procédure.

Remarque Si vous ne l'avez pas encore fait, copiez la configuration de haute disponibilité du périphérique principal dans le presse-papiers. Il est beaucoup plus facile de configurer le périphérique secondaire à l'aide du copier/coller que de saisir manuellement les données.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Dans la partie droite du résumé du périphérique, cliquez sur **Configure** (Configurer) à côté du groupe **High Availability** (Haute disponibilité).

Si vous configurez la haute disponibilité pour la première fois sur le périphérique, le groupe ressemblerait à ce qui suit.



Étape 3 Sur la page High Availability (Haute disponibilité), cliquez sur la case **Secondary Device** (Périphérique secondaire).

Étape 4 Effectuez l'une des opérations suivantes :

- **Méthode facile** : cliquez sur le bouton **Paste from Clipboard** (Coller à partir du presse-papiers), collez la configuration et cliquez sur **OK**. Cela mettra à jour les champs avec les valeurs appropriées, que vous pourrez ensuite vérifier.
- **Méthode manuelle** : configurez les liens de basculement et de basculement avec état directement. Saisissez exactement les mêmes paramètres sur le périphérique secondaire que vous avez saisis sur le périphérique principal.

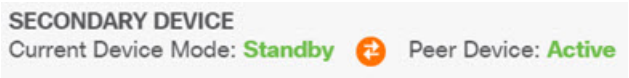
Étape 5 Si vous avez configuré une **clé de chiffrement IPSec** sur le périphérique principal, saisissez exactement la même clé pour le périphérique secondaire.

Étape 6 Cliquez sur **Activate HA** (Activer HA).

Le système déploie immédiatement la configuration sur le périphérique. Vous n'avez pas besoin de démarrer une tâche de déploiement. Si vous ne voyez pas de message indiquant que votre configuration a été enregistrée et que le déploiement est en cours, faites défiler la page vers le haut pour voir les messages d'erreur.

Une fois la configuration terminée, vous recevez un message indiquant que vous avez configuré la haute disponibilité. Cliquez sur **Got It** (J'ai compris) pour supprimer le message.

À ce stade, vous devriez être sur la page High Availability (haute disponibilité), et l'état de votre périphérique doit indiquer qu'il s'agit du périphérique secondaire. Si la jonction avec le périphérique principal a réussi, le périphérique se synchronisera avec le périphérique principal et, finalement, le mode devrait être Standby (veille) et l'homologue devrait être Active (actif).



Remarque
Les interfaces sélectionnées ne sont pas configurées directement. Toutefois, si vous saisissez **show interface** dans l'interface de ligne de commande, vous constaterez que les interfaces utilisent les adresses IP spécifiées. Les interfaces sont nommées « failover-link » et, si vous configurez une liaison d'état distincte, « stateful-failover-link ».

Configurer les critères de basculement pour la surveillance de l'intégrité

Les unités dans une configuration à haute disponibilité se surveillent elles-mêmes pour l'intégrité globale et l'intégrité des interfaces.

Les critères de basculement définissent les mesures de surveillance d'intégrité qui déterminent si un homologue est défaillant. Si l'homologue actif est l'unité qui ne respecte pas les critères, il déclenche un basculement vers l'unité de secours. Si l'homologue de secours est l'unité qui ne respecte pas les critères, elle est marquée comme ayant échoué et n'est pas disponible pour le basculement.

Vous pouvez configurer les critères de basculement sur le périphérique actif uniquement.

Le tableau suivant présente les événements déclencheurs de basculement et la synchronisation de détection des défaillances.

Tableau 8 : Délais de basculement en fonction des critères de basculement

Événement déclencheur de basculement	Minimum	Par défaut	Maximum
L'unité active perd de l'alimentation ou arrête le fonctionnement normal.	800 milliseconde	15 secondes	45 secondes
Le lien physique de l'interface de l'unité active est en panne.	500 millisecondes	5 secondes	15 secondes
L'interface de l'unité active est en service, mais un problème de connexion entraîne des tests d'interface.	5 secondes	25 secondes	75 secondes

Les rubriques suivantes expliquent comment personnaliser les critères de surveillance de l'intégrité du basculement et comment le système teste les interfaces.

Configurer les critères de basculement de la surveillance de l'intégrité des unités homologues

Chaque unité dans une configuration à haute disponibilité détermine l'intégrité de l'autre unité en surveillant le lien 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. La mesure que prend le périphérique dépend de la réponse de l'autre unité.

- Si le périphérique reçoit une réponse sur le lien de basculement, il ne bascule pas.
- Si le périphérique 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. Le lien 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 le lien de basculement est inactif.
- Si le périphérique ne reçoit de réponse sur aucune interface, l'unité en veille passe en mode actif et classe l'autre unité comme en panne.

Vous pouvez configurer l'interrogation et le délai de rétention des messages Hello.

Procédure

Étape 1 Sur le périphérique actif, cliquez sur **Device** (Périphérique).

Étape 2 Cliquez sur le lien **High Availability** (Haute disponibilité) sur le côté droit du résumé du périphérique.

Les critères de basculement sont répertoriés dans la colonne de droite de la page High Availability (Haute disponibilité).

Étape 3 Définissez la **Peer Timing Configuration** (Configuration de synchronisation de l'unité homologue).

Ces paramètres déterminent la vitesse à laquelle le périphérique actif peut basculer vers le périphérique en veille. Avec un temps de sondage plus court, le périphérique peut détecter une défaillance et déclencher le basculement plus rapidement. Cependant, une détection plus rapide peut entraîner des basculements inutiles lorsque le réseau est temporairement congestionné. Les paramètres par défaut sont appropriés pour la plupart des situations.

Si une unité ne reçoit pas de paquet hello sur l'interface de basculement pendant une période de sondage, des tests supplémentaires sont effectués sur les interfaces restantes. S'il n'y a toujours aucune réponse de l'unité homologue pendant le délai de maintien, l'unité est considérée comme défaillante et, si l'unité défaillante est l'unité active, l'unité en veille prend le relais comme unité active.

- **Poll Time (Délai de sondage)** : durée entre les messages hello. Saisissez de 1 à 15 secondes ou de 200 à 999 millisecondes. La valeur par défaut est de 1 seconde.
- **Hold Time** (Délai de rétention) : durée pendant laquelle une unité doit recevoir un message hello sur le lien de basculement, après quoi l'unité homologue est déclarée en panne. Le délai de rétention doit être au moins 3 fois supérieur au délai de sondage. Saisissez de 1 à 45 secondes ou de 800 à 999 millisecondes. La valeur par défaut est de 15 secondes.

Étape 4 Cliquez sur **Save** (Enregistrer).

Configurer les critères de basculement pour la surveillance de l'intégrité des interfaces

Vous pouvez surveiller jusqu'à 211 interfaces, selon le modèle de votre périphérique. Vous devez surveiller les interfaces importantes. Par exemple, les interfaces qui assurent le débit entre les réseaux importants. Surveillez une interface uniquement si vous configurez des adresses IP de secours pour celle-ci et si l'interface doit toujours être opérationnelle.

Lorsqu'une unité ne reçoit pas de messages Hello sur une interface surveillée pendant 2 périodes de sondage, elle exécute des tests d'interface. Si tous les tests d'interface échouent pour une interface, mais que cette même interface sur l'autre unité continue de transmettre correctement le trafic, l'interface est considérée comme défaillante. Si le seuil pour les interfaces défaillantes est atteint, un basculement se produit. Si une interface échoue sur les deux unités, les deux interfaces passent à l'état « Unknown » (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 périphérique défaillant repasse en mode veille si le seuil de défaillance d'interface n'est plus atteint.

Vous pouvez surveiller l'état de l'interface à haute disponibilité à partir de l'interface de ligne de commande ou de la console d'interface de ligne de commande en utilisant la commande **show monitor-interface**. Pour en savoir plus, consultez Surveillance de l'état pour les interfaces surveillées par la haute disponibilité, à la page 243.

Remarque Lorsqu'une interface tombe en panne, elle est toujours considérée comme un problème d'unité pour le basculement. Si l'unité détecte qu'une interface est en panne, le basculement se produit immédiatement (si vous conservez le seuil par défaut de 1 interface), sans attendre le délai de rétention de l'interface. Le délai de rétention de l'interface n'est utile que lorsque l'unité considère que son état est OK, bien qu'elle ne reçoive pas de paquets Hello de l'homologue.

Avant de commencer

Par défaut, toutes les interfaces physiques nommées sont sélectionnées pour la surveillance à haute disponibilité. Ainsi, vous devez désactiver la surveillance sur les interfaces physiques moins critiques. Pour les sous-interfaces ou les groupes de ponts, vous devez activer manuellement la surveillance.

Pour désactiver complètement la surveillance des interfaces et empêcher le basculement en raison d'une défaillance d'interface, assurez-vous simplement qu'aucune interface n'est activée pour la surveillance à haute disponibilité.

Procédure

Étape 1 Sur le périphérique actif, cliquez sur **Device** (Périphérique).

Étape 2 Cliquez sur le lien **High Availability** (Haute disponibilité) sur le côté droit du résumé du périphérique.

Les critères de basculement sont répertoriés dans la colonne de droite de la page High Availability (Haute disponibilité).

Étape 3 Définissez le **Interface Failure Threshold** (Seuil de défaillance de l'interface).

Si le nombre d'interfaces défaillantes atteint le seuil, l'unité se marque comme défaillante. Si l'unité est l'unité active, elle bascule vers l'unité de secours. Si l'unité est l'unité de secours, en se notant comme défaillante, l'unité active ne considérera pas l'unité comme disponible pour le basculement.

Lors de la définition de ces critères, tenez compte du nombre d'interfaces que vous surveillez. Par exemple, si vous activez la surveillance sur seulement 2 interfaces, le seuil de 10 interfaces ne sera jamais atteint. Vous configurez la surveillance pour une interface en sélectionnant l'option **Enable for HA Monitoring** (Activer la surveillance à haute disponibilité) sous l'onglet **Advanced Options** (Options avancées) lors de la modification des propriétés de l'interface.

Par défaut, l'unité se marque d'elle-même comme défaillante si une interface surveillée tombe en panne.

Vous pouvez définir le seuil de défaillance de l'interface en sélectionnant l'une des options **Failover Criteria** (Critère de basculement) suivantes :

- **Number of failed interfaces exceeds** (Nombre d'interfaces défaillantes supérieur à) : saisissez le nombre brut d'interfaces. La valeur par défaut est 1. Le maximum dépend en fait du modèle de périphérique et peut varier, mais vous ne pouvez pas saisir plus de 211. Si vous utilisez ce critère, vous obtiendrez une erreur de déploiement si vous saisissez un nombre supérieur à celui que le périphérique prend en charge. Essayez un nombre plus petit ou utilisez plutôt un pourcentage.
- **Percentage of failed interfaces exceed**s (Le pourcentage d'interfaces défaillantes dépasse) : saisissez un nombre de 1 à 100. Par exemple, si vous saisissez 50 % et que vous surveillez 10 interfaces, le périphérique se marque lui-même comme comme défaillant si 5 interfaces échouent.

Étape 4 Définissez **Interface Timing Configuration** (Configuration de la temporisation de l'interface)

Ces paramètres déterminent la vitesse à laquelle l'appareil actif peut déterminer si une interface est défaillante. Étant donné que le délai de sondage est plus rapide, l'appareil peut détecter plus rapidement les défaillances d'interface. Cependant, une détection plus rapide peut signifier que les interfaces occupées sont marquées comme étant défaillantes alors qu'elles fonctionnent correctement, ce qui peut entraîner des basculements inutilement fréquents. Les paramètres par défaut sont appropriés pour la plupart des situations.

Si une liaison d'interface est en panne, le test d'interface n'est pas effectué et l'unité de secours peut devenir active en une seule période d'interrogation d'interface si le nombre d'interfaces défaillantes atteint ou dépasse le seuil de basculement d'interface configuré.

- **Poll Time** (Délai de sondage) : la fréquence à laquelle les paquets Hello sont envoyés sur les interfaces de données. Saisissez de 1 à 15 secondes ou de 500 à 999 millisecondes. La valeur par défaut est de 5 secondes.

- **Hold Time** (Temps de rétention : la durée entre le moment où un paquet Hello est manqué et le moment où l'interface est marquée comme défaillante. Saisissez entre 5 et 75 secondes. Vous ne pouvez pas saisir une valeur de délai de rétention inférieure à 5 fois le délai de sondage.

Étape 5 Cliquez sur **Save** (enregistrer).

Étape 6 Activez la surveillance à haute disponibilité pour chaque interface que vous souhaitez surveiller.

a) Choisissez **Device (Périphérique)** > **Interfaces**.

Si une interface est surveillée, la colonne Monitor for HA (Surveillance HA) indique Enabled (Activé).

b) Cliquez sur l'icône de modification ( ) d'une interface dont vous souhaitez modifier l'état de surveillance.

Vous ne pouvez pas modifier les interfaces de basculement ou de basculement dynamique. La surveillance des interfaces ne s'applique pas à elles.

c) Cliquez sur l'onglet **Advanced Options** (Options avancées).

d) Cochez ou décochez la case **Enable for HA Monitoring** (Activer la surveillance à haute disponibilité) selon vos préférences.

e) Cliquez sur **OK**.

Étape 7 (Facultatif, mais conseillé.) Configurez les adresses IP de secours et les adresses MAC pour les interfaces surveillées. Consultez Configurer les adresses IP et MAC de secours, à la page 227.

Comment le système teste l'intégrité de l'interface

Le système teste en continu les interfaces que vous supervisez afin de vérifier leur état de haute disponibilité. L'adresse utilisée pour le test d'une interface dépend des types d'adresses que vous configurez :

- Si une interface a des adresses IPv4 et IPv6 configurées, le périphérique utilise les adresses IPv4 pour effectuer la surveillance de l'intégrité.
- Si une interface n'a que des adresses IPv6 configurées, le périphérique 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, le périphérique utilise l'adresse de tous les nœuds IPv6 (FE02::1).

Le système effectue les tests suivants sur chaque unité :

1. Test de liaison (Active/En panne) : test de l'état de l'interface. Si le test Link Up/Down (liaison active/désactivée) indique que l'interface est en panne, l'unité la considère comme défaillante. Si l'état est Up (activé), l'unité exécute le Network Activity test (test d'activité réseau).
2. Test d'activité réseau : test d'activité réseau reçu. Le but de ce test est de générer le trafic réseau à l'aide des messages LANTEST pour déterminer quelle unité (le cas échéant) a échoué. Au début du test, chaque unité efface son nombre de paquets reçus pour ses interfaces. Dès qu'une unité reçoit des paquets pendant le test (jusqu'à 5 secondes), l'interface est considérée comme opérationnelle. 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. Si aucune des unités ne reçoit de trafic, l'unité démarre le test ARP.
3. Test ARP : lecture du cache ARP de l'unité pour les 2 dernières entrées. Une à la fois, l'unité envoie des requêtes ARP à ces périphériques, pour tenter de relancer le trafic réseau. Après chaque demande, l'unité compte tout le trafic reçu pendant 5 secondes maximum. Si le trafic est reçu, l'interface est considérée comme opérationnelle. Si aucun trafic n'est reçu, une demande ARP est envoyée au périphérique suivant. Si à la fin de la liste aucun trafic n'a été reçu, l'unité démarre le test ping.

4. Test de ping de diffusion : test de ping qui consiste à envoyer une demande de ping de diffusion. L'unité compte ensuite tous les paquets reçus pendant un maximum de 5 secondes. Si des paquets sont reçus à tout moment pendant cet intervalle, l'interface est considérée comme opérationnelle et le test s'arrête. Si aucun trafic n'est reçu, les tests recommencent avec le test ARP.

Configurer les adresses IP et MAC de secours

Lorsque vous configurez vos interfaces, vous pouvez spécifier une adresse IP active et une adresse IP de secours sur le même réseau. 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.

1. Lorsque l'unité principale bascule, l'unité secondaire adopte les adresses IP et MAC de l'unité principale et commence à transmettre le trafic.
2. L'unité qui est maintenant en état de veille prend le relais des adresses IP et MAC de secours.

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.

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. Cependant, 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.

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. Vous pouvez configurer manuellement des adresses MAC virtuelles.

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. Appareil FTD 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.

Procédure

Étape 1 Choisissez **Device (Périphérique)** > **Interfaces**.

Vous devez au moins configurer des adresses IP et MAC de secours pour les interfaces que vous surveillez pour la haute disponibilité. Si une interface est surveillée, la colonne Monitor for HA (Surveillance HA) indique Enabled (Activé).

Étape 2 Cliquez sur l'icône de modification ( ) de l'interface dont vous souhaitez configurer les adresses de secours.

Vous ne pouvez pas modifier les interfaces de basculement ou de basculement dynamique. Vous définissez les adresses IP de ces interfaces lorsque vous configurez la haute disponibilité.

Étape 3 Configurez les adresses IP de secours dans les onglets **IPv4 Address** (Adresse IPv4) et **IPv6 Address** (Adresse IPv6).

L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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. Configurez des adresses de secours pour chaque version IP utilisée.

Étape 4 Cliquez sur l'onglet **Advanced Options** (Options avancées) et configurez les adresses MAC.

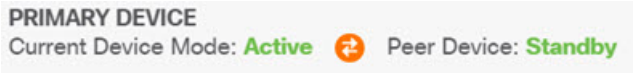
Par défaut, le système utilise l'adresse MAC gravée dans la carte d'interface réseau (NIC) pour l'interface. Ainsi, toutes les sous-interfaces d'une interface utilisent la même adresse MAC. Vous pouvez donc créer des adresses uniques par sous-interface. Des adresses MAC actives/en attente configurées manuellement sont également recommandées si vous configurez la haute accessibilité. La définition des adresses MAC permet de maintenir la cohérence du réseau en cas de basculement.

- **MAC Address** (Adresse MAC) : l'adresse Media Access Control au format H.H.H, où H correspond à une valeur hexadécimale de 16 bits. Par exemple, vous devez entrer l'adresse MAC 00-0C-F1-42-4C-DE comme 000C.F142.4CDE. L'adresse MAC ne doit pas avoir le bit de multidiffusion activé; autrement dit, le deuxième chiffre hexadécimal à partir de la gauche ne peut pas être un nombre impair.
- **Standby MAC Address** (adresse MAC en veille) : À utiliser avec la haute disponibilité. 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 5 Cliquez sur **OK**.

Vérifier la High Availability Configuration (Configuration de la haute disponibilité)

Après avoir terminé la configuration de la haute disponibilité, vérifiez que l'état du périphérique indique que les deux périphériques sont opérationnels et en mode actif/en veille.



Vous pouvez vérifier que la configuration de haute disponibilité fonctionne en suivant cette procédure.

Procédure

Étape 1 Testez que votre unité active transmet le trafic comme prévu en utilisant FTP (par exemple) pour envoyer un fichier entre des hôtes sur différentes interfaces.

Testez au minimum les connexions d'un poste de travail vers les systèmes connectés à chacune des interfaces configurées.

Étape 2 Basculez de mode de sorte que l'unité active devienne l'unité de secours en effectuant l'une des opérations suivantes :

- Dans le Gestionnaire de périphériques de pare-feu, sélectionnez **Switch Mode** (Changer de mode) à partir du menu d'engrenage sur la page **Device (Périphérique)** > **High Availability (Haute disponibilité)**.
- Dans l'interface de ligne de commande de l'unité active, saisissez **no failover active**.

Étape 3 Répétez les tests de connexion pour vérifier que vous pouvez établir les mêmes connexions par l'intermédiaire de l'autre unité de la paire de haute disponibilité.

Si le test échoue, vérifiez que vous avez connecté les interfaces de l'unité aux mêmes réseaux que les interfaces équivalentes sur l'autre unité.

Vous pouvez voir l'état de HA à partir de la page High Availability (Haute disponibilité). Vous pouvez également utiliser l'interface de ligne de commande ou la console d'interface de ligne de commande de l'unité et saisir la commande **show failover** pour vérifier l'état du basculement. Utilisez également la commande **show interface** pour vérifier la configuration d'interface pour les interfaces utilisées dans les tests de connexion qui ont échoué.

Si ces actions ne détectent pas le problème, il existe d'autres étapes que vous pouvez suivre. Consultez Dépannage de la haute disponibilité (basculement), à la page 244.

Étape 4 Lorsque vous avez terminé, vous pouvez basculer de mode pour rétablir l'état actif de l'unité d'origine qui était active.

Gérer la haute disponibilité

Vous pouvez gérer une paire à haute disponibilité en cliquant sur le lien **High Availability** (Haute disponibilité) sur la page **Device Summary** (Résumé des périphériques).



La page Haute disponibilité comprend les éléments suivants :

- **État du rôle et du mode** : la zone d'état gauche indique si le périphérique est le Primary (Primaire) ou le Secondary (Secondaire) du groupe. Le mode indique si ce périphérique est actif ou en veille, ou si la haute disponibilité a été suspendue ou si le périphérique attend de rejoindre le périphérique homologue. Il affiche également l'état du périphérique homologue, qui peut être actif, en veille, suspendu ou en panne. Par exemple, lorsque vous êtes connecté au périphérique principal et qu'il s'agit également du périphérique actif, et que le périphérique secondaire est intègre et prêt à basculer si nécessaire, l'état ressemblerait à ce qui suit. Vous pouvez cliquer sur l'icône entre les homologues pour obtenir des informations sur l'état de la synchronisation de la configuration entre les périphériques.

- **Dernière raison de l'échec** : si la configuration de la haute disponibilité (HA) échoue pour une raison quelconque, comme le périphérique actif devient indisponible et bascule vers le périphérique de secours, la dernière raison de l'échec est indiquée sous les informations d'état du rôle et du mode. Ce message est dérivé de l'historique de basculement.
- Lien **Failover History** (Historique de basculement) : cliquez sur ce lien pour voir l'historique détaillé de l'état des périphériques de la paire. Le système ouvre la console d'interface de ligne de commande et exécute la commande **show failover history details**.
- Lien **Deployment History** (Historique de déploiement) : cliquez sur ce lien pour accéder au journal d'audit avec les événements filtrés pour afficher uniquement les tâches de déploiement.

- **Gear button** (Bouton d'engrenage) : cliquez sur ce bouton pour effectuer des actions sur les appareils.
  - **Suspend HA** (Suspendre la haute disponibilité)/**Resume HA** (Reprendre la haute disponibilité) : la suspension de la haute disponibilité empêche les périphériques de fonctionner en tant que paire à haute disponibilité sans supprimer la configuration de haute disponibilité. Vous pouvez ultérieurement reprendre, c'est-à-dire réactiver, la haute disponibilité sur les périphériques. Pour de plus amples renseignements, consultez la section Suspendre et reprendre la haute disponibilité, à la page 230.
  - **Break HA (Rupture de la haute disponibilité)** : la rupture de la haute disponibilité supprime la configuration de haute disponibilité des deux périphériques et les ramène aux périphériques autonomes. Pour de plus amples renseignements, consultez la section Rupture de la haute disponibilité, à la page 232.
  - **Switch Mode** (Mode de commutation) : le mode de commutation vous permet de forcer un périphérique actif à passer en veille ou un périphérique en veille à devenir actif, selon le périphérique à partir duquel vous effectuez l'action. Pour de plus amples renseignements, consultez la section Commutation des homologues actifs et de secours (forcer le basculement), à la page 233.
- **High Availability Configuration** (Configuration de la haute disponibilité) : ce panneau affiche la configuration de la paire de basculement. Cliquez sur le bouton **Copy to Clipboard** (Copier dans le presse-papier) pour charger les informations dans le presse-papier, à partir duquel vous pouvez les coller dans la configuration du périphérique secondaire. Vous pouvez également le copier dans un autre fichier pour vos enregistrements. Ces informations n'affichent pas si vous avez défini une clé de chiffrement IPsec.

Remarque La configuration d'interface pour la haute disponibilité n'est pas reflétée dans la page Interfaces (**Device (appareil)** > **Interfaces**). Vous ne pouvez pas modifier les interfaces que vous utilisez dans une configuration à haute disponibilité.

- **Failover Criteria** (Critères de basculement) : ce panneau comprend les paramètres qui déterminent les critères d'intégrité utilisés pour évaluer si l'unité active est défaillante et si l'unité de secours doit devenir l'unité active. Ajustez ces critères afin d'obtenir les performances de basculement requises dans votre réseau. Pour de plus amples renseignements, consultez la section Configurer les critères de basculement pour la surveillance de l'intégrité, à la page 222.

Les rubriques suivantes expliquent diverses tâches de gestion liées à une configuration à haute disponibilité.

Suspendre et reprendre la haute disponibilité

Vous pouvez suspendre une unité dans une paire à haute disponibilité. C'est utile dans les cas suivants :

- Les deux unités sont dans une situation active-active et la correction de la communication sur la liaison de basculement ne résout pas le problème.
- Vous souhaitez effectuer le dépannage d'une unité active ou en veille et que vous ne souhaitez pas que les unités basculent pendant ce temps.
- Vous souhaitez empêcher le basculement lors de l'installation d'une mise à niveau logicielle sur le périphérique de secours.

Lorsque vous suspendez la haute disponibilité, vous empêchez la paire de périphériques de se comporter comme une unité de basculement. Le périphérique actuellement actif reste actif et gère toutes les connexions d'utilisateur. Cependant, les critères de basculement ne sont plus surveillés et le système ne basculera jamais sur le périphérique maintenant en pseudo-veille. Le périphérique en veille conservera sa configuration, mais il restera inactif.

la différence clé entre la suspension de la haute disponibilité et l'arrêt de la haute disponibilité est que sur un périphérique à haute disponibilité interrompu, la configuration à haute disponibilité est conservée. Lorsque vous annulez la haute disponibilité, la configuration est effacée. Ainsi, vous avez la possibilité de réactiver la haute disponibilité sur un système interrompu, ce qui active la configuration existante et fait fonctionner les deux périphériques à nouveau comme paire de basculement.

La suspension de la haute disponibilité sur l'unité active suspend la haute disponibilité sur l'unité active et l'unité en veille. Si vous la suspendez sur l'unité en veille, elle est suspendue sur l'unité en veille uniquement, mais l'unité active ne tentera pas de basculer vers une unité suspendue.

Vous pouvez reprendre une unité uniquement si elle est à l'état Suspended (Suspendu). L'unité négociera l'état actif/en veille avec l'unité homologue.



Remarque Si nécessaire, vous pouvez suspendre la haute disponibilité depuis l'interface de ligne de commande en saisissant la commande **configure high-availability suspend**. Pour réactiver la haute disponibilité, saisissez **configure high-availability resume**.

Avant de commencer

Si vous suspendez la haute disponibilité par l'intermédiaire du Gestionnaire de périphériques de pare-feu, elle reste suspendue jusqu'à ce que vous la repreniez, même si vous rechargez l'unité. Cependant, si vous la suspendez au moyen de la console d'interface en ligne de commande, il s'agit d'un état temporaire et, lors du rechargement, l'unité reprend automatiquement la configuration de haute disponibilité et négocie l'état actif/en veille avec l'homologue.

Si vous suspendez la haute disponibilité sur l'unité en veille, vérifiez si l'unité active exécute actuellement une tâche de déploiement. Si vous changez de mode alors qu'une tâche de déploiement est en cours, la tâche échouera et vous perdrez vos modifications de configuration.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Cliquez sur le lien **High Availability** (Haute disponibilité) sur le côté droit du résumé du périphérique.

Étape 3 Choisissez la commande appropriée dans l'icône en forme d'engrenage ( ).

- **Suspend HA** (Suspendre la haute disponibilité) : vous êtes invité à confirmer l'action. Lisez le message et cliquez sur **OK**. L'état de la haute disponibilité devrait indiquer que le périphérique est en mode Suspended (Suspendu).

- **Resume HA** (Reprendre la haute disponibilité) : vous êtes invité à confirmer l'action. Lisez le message et cliquez sur **OK**. L'état de haute disponibilité devrait redevenir normal, soit actif, soit en veille, après que l'unité a négocié avec l'homologue.

Rupture de la haute disponibilité

Si vous ne souhaitez plus que les deux périphériques fonctionnent en tant que paire à haute disponibilité, vous pouvez interrompre la configuration à haute disponibilité. Lorsque vous annulez la haute disponibilité, chaque périphérique devient un périphérique autonome. Leurs configurations sont modifiées comme suit :

- Le périphérique actif conserve la configuration complète telle qu'elle était avant l'interruption, avec la configuration à haute disponibilité supprimée.
- Le périphérique de secours voit toute la configuration d'interface supprimée en plus de la configuration à haute disponibilité. Toutes les interfaces physiques sont désactivées, bien que les sous-interfaces ne soient pas désactivées. L'interface de gestion reste active, vous pouvez donc vous connecter au périphérique et le reconfigurer.



Remarque Vous pouvez également utiliser la ressource API BreakHAStatus (à partir de l'explorateur d'API) et utiliser l'attribut **interfaceOption** pour demander au système de reconfigurer les interfaces du périphérique en veille à l'aide des adresses IP en veille. Vous devez utiliser l'API si vous souhaitez ce résultat ; sinon, Gestionnaire de périphériques de pare-feu désactive toujours les interfaces. Notez que le système reconfigure les adresses IP, mais ne reconfigure pas toutes les options d'interface, de sorte que le trafic peut ne pas se comporter comme prévu tant que vous n'avez pas déployé les modifications après l'interruption.

La façon dont l'interruption affecte réellement les unités dépend de l'état de chaque unité lorsque vous effectuez l'interruption.

- Si les unités sont dans un état actif/en veille intègre, cassez la haute disponibilité de l'unité active. Cela supprimera la configuration à haute disponibilité des deux périphériques de la paire à haute disponibilité. Si vous souhaitez interrompre la haute disponibilité sur l'unité de secours uniquement, vous devez vous y connecter et d'abord suspendre la haute disponibilité, puis vous pourrez interrompre la haute disponibilité.
- Si l'unité de secours est en état suspendu ou en panne, l'interruption de la haute disponibilité de l'unité active supprime la configuration à haute disponibilité de l'unité active uniquement. Vous devez vous connecter à l'unité de secours et également interrompre la haute disponibilité sur cette unité.
- Si les homologues négocient toujours la haute disponibilité ou synchronisent leur configuration, vous ne pouvez pas interrompre la haute disponibilité. Attendez que la négociation ou la synchronisation soit terminée ou expire. Si vous pensez que les systèmes sont bloqués dans cet état, vous pouvez suspendre la haute disponibilité, puis l'interrompre.

Remarque Lorsque vous utilisez Gestionnaire de périphériques de pare-feu, vous ne pouvez pas interrompre la haute disponibilité de l'interface de ligne de commande à l'aide de la commande **configure high-availability disable**.

Avant de commencer

Pour des résultats idéaux, mettez les périphériques dans un état actif/en veille et effectuez cette action à partir du périphérique actif.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Cliquez sur le lien **High Availability** (Haute disponibilité) sur le côté droit du résumé du périphérique.

Étape 3 Dans l'icône en forme d'engrenage ( ), choisissez **Break HA** (Rompre la haute disponibilité).

Étape 4 Lisez le message de confirmation, décidez de sélectionner l'option de désactivation des interfaces, puis cliquez sur **OK**.

Vous devez sélectionner l'option de désactivation des interfaces si vous rompez la haute disponibilité à partir de l'unité de secours.

Le système déploie immédiatement vos modifications sur ce périphérique et le périphérique homologue (si possible). Cela peut prendre quelques minutes pour que le déploiement sur chaque périphérique et pour que chaque périphérique devienne indépendant.

Commutation des homologues actifs et de secours (forcer le basculement)

Vous pouvez permuter les modes actif / en veille pour une paire à haute disponibilité opérationnelle, c'est-à-dire qu'un homologue est actif, l'autre est en veille. Par exemple, si vous installez une mise à niveau logicielle, vous pouvez mettre l'unité active en veille afin que la mise à niveau n'ait pas d'incidence sur le trafic des utilisateurs.

Vous pouvez changer de mode à partir de l'unité active ou en veille, mais l'unité homologue doit fonctionner du point de vue de l'autre unité. Vous ne pouvez pas changer de mode si une unité est suspendue (vous devez d'abord reprendre la haute disponibilité) ou en échec.

Remarque Au besoin, vous pouvez basculer entre les modes actif et en veille à partir de la console d'interface en ligne de commande. À partir de l'unité en veille, dans la console d'interface en ligne de commande, saisissez la commande **failover active**. À partir de l'unité active, entrez la commande **no failover active**.

Avant de commencer

Avant de changer de mode, vérifiez que l'unité active n'est pas en cours de tâche de déploiement. Attendez que le déploiement soit terminé avant de changer de mode.

Si l'unité active a des modifications non déployées en attente, déployez-les avant de changer de mode. Sinon, vous perdrez vos modifications si vous exécutez une tâche de déploiement à partir de la nouvelle unité active.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Cliquez sur le lien **High Availability** (Haute disponibilité) sur le côté droit du résumé du périphérique.

Étape 3 À partir de l'icône en forme d'engrenage (⚙), choisissez **Switch Mode** (Mode de commutation).

Étape 4 Lisez le message de confirmation et cliquez sur **OK**.

Le système force le basculement de sorte que l'unité active passe en veille et que l'unité en veille devient la nouvelle unité active.

Préservation des modifications de configuration non déployées après un basculement

Lorsque vous apportez des modifications à la configuration des unités d'une paire à haute disponibilité, vous modifiez la configuration sur l'unité active. Vous déployez ensuite vos modifications, et les unités active et en veille sont mises à jour avec la nouvelle configuration. Peu importe que l'unité active soit le périphérique principal ou secondaire.

Cependant, les modifications non déployées ne sont pas synchronisées entre les unités. Toutes les modifications non déployées sont disponibles uniquement sur l'unité où vous avez apporté ces modifications.

Ainsi, si un basculement se produit lorsque vous avez des modifications non déployées, ces modifications ne sont pas disponibles sur la nouvelle unité active. Les modifications restent cependant en place sur l'unité qui est maintenant en veille.

Pour récupérer vos modifications non déployées, vous devez changer de mode pour forcer un basculement et faire revenir l'autre unité à l'état actif. Lorsque vous vous connectez à l'unité nouvellement active, vos modifications non déployées sont disponibles et vous pouvez les déployer. Utilisez la commande **Switch Modes** (changer de mode) dans le menu d'engrenage des paramètres de **High Availability** (haute disponibilité) (⚙).

Veuillez garder à l'esprit les éléments suivants :

- Si vous déployez des modifications à partir de l'unité active alors qu'il y a des modifications non déployées sur l'unité en veille, les modifications non déployées sur l'unité en veille seront effacées. Vous ne pourrez pas les récupérer.
- Lorsqu'une unité de secours rejoint une paire à haute accessibilité, toutes les modifications non déployées sur l'unité de secours sont effacées. La configuration est synchronisée chaque fois qu'une unité rejoint ou rejoint la paire.

- Si l'unité qui contient les modifications non déployées a échoué de manière catastrophique et que vous avez dû la remplacer ou la recréer, vos modifications non déployées sont définitivement perdues.

Modification des licences et de l'enregistrement en mode de haute disponibilité

Les unités de la paire à haute disponibilité doivent avoir les mêmes licences et le même statut d'enregistrement. Pour apporter des modifications :

- Vous activez ou désactivez les licences facultatives sur l'unité active. Puis vous déployez la configuration et l'unité de secours demande (ou libère) les licences nécessaires. Lorsque vous activez des licences, vous devez vous assurer que votre compte Cisco Smart Software Manager dispose de suffisamment de licences, sinon vous pourriez vous retrouver avec une unité conforme alors que l'autre unité est non conforme.
- Vous enregistrez ou annulez l'enregistrement des unités séparément. Pour fonctionner correctement, les unités doivent être en mode d'évaluation ou enregistrées. Si les périphériques sont enregistrés, ils peuvent être enregistrés dans différents comptes Cisco Smart Software Manager, mais les comptes doivent avoir le même état pour le paramètre de fonctionnalité de contrôle de l'exportation : activés ou désactivés. Vous ne pouvez pas déployer les modifications de configuration si les unités ont un état d'enregistrement incohérent.

Modification de la clé de chiffrement IPsec à haute disponibilité ou de la configuration à haute disponibilité

Vous pouvez modifier n'importe quel critère de basculement en vous connectant à l'unité active, en effectuant vos modifications et en les déployant.

Toutefois, si vous devez modifier la clé de chiffrement IPsec utilisée sur vos liaisons de basculement, ou modifier les interfaces ou les adresses IP pour les liaisons de basculement ou de basculement dynamique, vous devez d'abord interrompre la configuration à haute disponibilité. Vous pouvez ensuite reconfigurer les unités principale et secondaire avec la nouvelle clé de chiffrement ou les paramètres de basculement ou de liaison de basculement dynamique.

Marquer une unité défaillante comme saine

Une unité dans une configuration à haute disponibilité peut être marquée comme défaillante en raison d'une surveillance régulière de l'intégrité. Si l'unité est saine, elle devrait revenir à l'état normal lorsqu'elle répond de nouveau aux exigences de surveillance de l'intégrité. Si vous voyez un périphérique sain échouer fréquemment, vous pouvez augmenter les délais d'expiration de pair, cesser de superviser certaines interfaces moins importantes, ou modifier les délais d'expiration de supervision des interfaces.

Vous pouvez forcer une unité défaillante à être vue comme saine en saisissant la commande **failover reset** à partir de l'interface de ligne de commande. Nous vous recommandons d'entrer la commande à partir de l'unité active, ce qui réinitialisera l'état de l'unité de secours. Vous pouvez afficher l'état de basculement de l'unité à l'aide des commandes **show failover** ou **show failover state**.

La restauration d'une unité défaillante à un état sans défaillance ne la rend pas automatiquement active. Les unités restaurées restent à l'état de secours jusqu'à ce qu'elles soient activées par le basculement (contraint ou normal).

La réinitialisation de l'état du périphérique ne résout pas les problèmes qui ont mené au marquage du périphérique comme défaillant. Si vous ne corrigez pas les problèmes, ou si vous relâchez vos délais d'expiration de supervision, le périphérique peut être marqué comme défaillant de nouveau.

Mise à niveau de la haute disponibilité Firewall Threat Defense

Utilisez cette procédure pour mettre à niveau des périphériques à haute disponibilité. Mettez-les à niveau un à la fois. Pour minimiser les perturbations, mettez toujours à niveau le serveur de secours. C'est-à-dire que vous mettez à niveau le serveur de secours actuel, changez de rôle, puis mettez à niveau le nouveau serveur de secours. Si vous devez mettre à jour FXOS, faites-le sur les deux châssis avant de mettre à niveau Firewall Threat Defense sur l'un ou l'autre. Encore une fois, mettez toujours à niveau le serveur de secours.

Mise en garde N'apportez pas et n'utilisez pas de modifications de configuration sur une unité pendant que l'autre est en cours de mise à niveau, ou vers une paire de versions mixte. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement pendant la mise à niveau. vous pourriez rendre le système inutilisé et nécessiter une réinitialisation. Vous pouvez annuler manuellement les mises à niveau majeures ou de maintenance en cours ou qui ont échoué, et réessayer les mises à niveau qui ont échoué. Si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Pour en savoir plus sur ces problèmes et d'autres que vous pouvez rencontrer pendant la mise à niveau, consultez Dépannage des mises à niveau de Threat Defense haute disponibilité, à la page 238.

Avant de commencer

Terminer la planification de la mise à niveau. Vérifiez que votre déploiement est intègre et communique correctement.

Astuces La planification de la mise à niveau commence par la lecture du Notes de version de Secure Firewall Threat Defense. Elle inclut ensuite la création de sauvegardes, l'obtention des paquets de mise à niveau et l'exécution des mises à niveau associées (comme FXOS pour Firepower 4100/9300). Elle comprend également la vérification des modifications de configuration nécessaires, de la préparation, de la vérification de l'espace disque et de la vérification des tâches en cours d'exécution et planifiées. Pour en savoir plus, consultez le informations sur la planification de la mise à niveau dans le Guide de mise à niveau de Cisco Firepower Threat Defense pour Firepower Device Manager, version 7.1.

Procédure

Étape 1 Connectez-vous à l'unité en veille.

Étape 2 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le volet des mises à jour (Updates).
Le volet de mise à niveau du système indique la version du logiciel en cours d'exécution et tout paquet de mise à niveau que vous avez déjà téléversé.

Étape 3 Téléverser le paquet de mise à niveau

Vous ne pouvez téléverser qu'un seul paquet. Si vous téléversez un nouveau fichier, il remplace l'ancien fichier. Assurez-vous que le paquet convient à votre version cible et au modèle de périphérique. Cliquez sur **Parcourir** ou sur **Remplacer le fichier** pour commencer le téléversement.

Une fois le téléversement terminé, le système affiche une boîte de dialogue de confirmation. Avant de cliquer sur **OK**, sélectionnez éventuellement **Exécuter la mise à niveau Immédiatement** pour et choisissez les options de restauration et la mise à niveau maintenant. Si vous effectuez une mise à niveau maintenant, il est particulièrement important d'avoir complété autant que possible la liste de contrôles avant mise à niveau (voir l'étape suivante).

Étape 4 Effectuer les vérifications finales préalables à la mise à niveau, y compris la vérification de l'état de préparation.

Consultez la liste de contrôles avant mise à niveau. Assurez-vous d'avoir effectué toutes les tâches pertinentes, en particulier les vérifications finales. Si vous n'exécutez pas la vérification de la préparation manuellement, elle s'exécute lorsque vous lancez la mise à niveau. Si la vérification échoue, la mise à niveau est annulée. Pour en savoir plus, consultez Exécution d'une vérification de l'état de préparation aux mises à niveau, à la page 825.

Étape 5 Cliquez sur **Upgrade Now** (Installer > Mettre à niveau maintenant) pour lancer le processus d'installation de la mise à niveau.

a) Choisissez les options de restauration.

Vous pouvez **Annuler automatiquement en cas d'échec de la mise à niveau et revenir à la version précédente**. Lorsque cette option est activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci qu'elle soit majeure ou de maintenance. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué.

b) Cliquez sur **Continuer** pour mettre à niveau et redémarrer le périphérique.

Vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la mise à niveau jusqu'à ce que le périphérique redémarre. La page comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, vous pouvez annuler manuellement ou tenter de nouveau la mise à niveau.

Le trafic est abandonné pendant la mise à niveau. Pour ISA 3000 uniquement, si vous avez configuré le contournement matériel pour une panne de courant, le trafic est abandonné pendant la mise à niveau, mais transmis sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.

Étape 6 Reconnectez-vous quand vous le pouvez et vérifiez la réussite de la mise à niveau.

La page Device Summary (Résumé du périphérique) affiche la version du logiciel actuellement exécutée et l'état de la haute disponibilité. Ne continuez pas tant que vous n'avez pas vérifié la réussite *et que* la haute disponibilité n'a pas été rétablie. Si la haute disponibilité reste suspendue après une mise à niveau réussie, consultez Dépannage des mises à niveau de Threat Defense haute disponibilité, à la page 238.

Étape 7 Mettez à niveau la deuxième unité.

a) Changer de rôle, rendant cet appareil actif : sélectionnez **Device** > **High Availability** (haute disponibilité du périphérique), puis sélectionnez **Switch Mode** (changer de mode) dans le menu déroulant ( ). Attendez que l'état de l'unité passe à actif et confirmez que le trafic circule normalement. Déconnectez-vous.

b) Mise à niveau : répétez les étapes précédentes pour vous connecter au nouveau serveur de secours, téléverser le paquet, mettre à niveau le périphérique, surveiller la progression et vérifier la réussite.

Étape 8 Examiner les rôles des périphériques.

Si vous avez défini des rôles privilégiés pour des périphériques précis, modifiez-les maintenant.

Étape 9 Connectez-vous à l'unité active.

Étape 10 Effectuer les tâches postérieures à la mise à niveau.

a) Mettez à jour les bases de données du système. Si les mises à jour automatiques ne sont pas configurées pour les règles de prévention des intrusions, VDB et GeoDB, mettez-les à jour maintenant.
b) Apportez toutes les modifications de configuration requises après la mise à niveau.
c) Déployez.

Dépannage des mises à niveau de Threat Defense haute disponibilité

Dépannage général de la mise à niveau

Ces problèmes peuvent se produire lorsque vous mettez à niveau un périphérique, qu'il soit autonome ou au sein d'une paire à haute disponibilité.

Erreurs relatives au paquet de mise à niveau

Pour trouver le bon paquet de mise à niveau, sélectionnez ou recherchez votre modèle sur Site d'assistance et de téléchargement Cisco, puis accédez à la page de téléchargement du logiciel pour la version appropriée. Les paquets de mise à niveau disponibles sont répertoriés avec les paquets d'installation, les correctifs rapides et les autres téléchargements applicables. Les noms des fichiers de paquet de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif), la version du logiciel et la version.

Les paquets de mise à niveau à partir de la version 6.2.1+ sont signés et se terminent par .sh.REL.tar. Ne décompressez pas les paquets de mise à niveau signés. Ne renommez pas les paquets de mise à niveau et ne les transférez pas par courriel.

Impossible d'atteindre le périphérique pendant la mise à niveau.

Les périphériques arrêtent de transmettre le trafic pendant la mise à niveau ou en cas d'échec de la mise à niveau. Avant d'effectuer la mise à niveau, assurez-vous que le trafic en provenance de votre emplacement n'a pas à traverser le périphérique lui-même pour accéder à l'interface de gestion du périphérique .

Le périphérique semble inactif ou ne répond pas pendant la mise à niveau.

Vous pouvez annuler manuellement les mises à niveau majeures et de maintenance en cours; voir Annulation ou nouvelle tentative des Firewall Threat Defense mises à niveau, à la page 827. Si le périphérique ne répond pas ou si vous ne pouvez pas annuler la mise à niveau, communiquez avec Centre d'assistance technique Cisco (TAC).



Mise en garde Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez *pas* manuellement pendant la mise à niveau. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image.

La mise à niveau a réussi, mais le système ne fonctionne pas comme vous le souhaitez.

Tout d'abord, assurez-vous que les informations en cache sont actualisées. N'actualisez pas simplement la fenêtre du navigateur pour vous reconnecter. Supprimez plutôt tout chemin « supplémentaire » de l'URL et reconnectez-vous à la page d'accueil; par exemple, http://threat-defense.exemple.com/.

Si vous continuez à rencontrer des problèmes et que vous devez revenir à une version majeure ou de maintenance antérieure, vous pourrez peut-être revenir à une version majeure ou de maintenance antérieure; voir Rétablissement Firewall Threat Defense en cours..., à la page 827. Si vous ne pouvez pas revenir en arrière, vous devez recréer l'image.

Échec de la mise à niveau.

Lorsque vous lancez une mise à niveau majeure ou de maintenance, utilisez la commande **Annuler automatiquement en cas d'échec de la mise à niveau...** Option d'annulation automatique pour choisir ce qui se passe en cas d'échec de la mise à niveau, comme suit :

- Annulation automatique activée (par défaut) : si la mise à niveau échoue, la mise à niveau est annulée et le périphérique revient automatiquement à l'état qu'il avait avant la mise à niveau. Corrigez les problèmes et réessayez.
- Annulation automatique désactivée : si la mise à niveau échoue, le périphérique reste tel qu'il est. Corrigez les problèmes et réessayez immédiatement, ou annulez manuellement la mise à niveau et réessayez ultérieurement.

Pour en savoir plus, consultez Annulation ou nouvelle tentative des Firewall Threat Defense mises à niveau, à la page 827. Si vous ne pouvez pas réessayer ou annuler, ou si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Dépannage de la mise à niveau haute disponibilité

Ces problèmes sont spécifiques aux mises à niveau à haute disponibilité.

La mise à niveau ne commencera pas sans le déploiement des modifications non validées.

Si vous obtenez un message d'erreur indiquant que vous devez déployer toutes les modifications non validées, même s'il n'y en a pas, connectez-vous à l'unité active (n'oubliez pas que vous devriez mettre à niveau l'unité de secours), créez des modifications mineures et déployez. Ensuite, annulez la modification, redéployez et réessayez la mise à niveau sur le serveur de secours.

Si cela ne fonctionne pas et que les unités exécutent des versions logicielles différentes par rapport aux recommandations, changez de rôle pour rendre l'unité en veille active, puis suspendez la haute disponibilité. Vous pouvez ensuite effectuer le déploiement à partir de l'unité active/suspendue, reprendre la haute disponibilité, puis changer encore les rôles pour mettre l'unité active en veille à nouveau. La mise à niveau devrait alors fonctionner.

Le déploiement à partir de l'unité active échoue pendant la mise à niveau de secours ou provoque une erreur de synchronisation de l'application.

Cela peut se produire si vous déployez à partir de l'unité active tandis que l'unité de secours est en cours de mise à niveau, ce qui n'est pas pris en charge. Procédez à la mise à niveau malgré l'erreur. Après avoir mis à niveau les deux unités, apportez les modifications de configuration requises et déployez à partir de l'unité active. L'erreur devrait être résolue.

Pour éviter ces problèmes, n'apportez pas et ne déployez pas de modifications de configuration sur une unité pendant que l'autre unité est en cours de mise à niveau, ou vers une paire de versions mixte.

Les modifications de configuration apportées depuis la mise à niveau seront perdues.

Si vous devez absolument apporter et déployer des modifications sur une paire de versions, vous devez apporter les modifications aux deux unités, sinon elles seront perdues après la mise à niveau de l'unité active de bas niveau.

La haute disponibilité est suspendue après la mise à niveau.

Après le redémarrage après la mise à niveau, la haute disponibilité est brièvement suspendue pendant que le système effectue certaines tâches automatisées finales, telles que la mise à jour des bibliothèques et le redémarrage de Snort. Vous êtes susceptible de le remarquer si vous vous connectez à la CLI *très* peu de temps après la mise à niveau. Si la haute disponibilité ne reprend pas d'elle-même après la fin de la mise à niveau et que Gestionnaire de périphériques de pare-feu est disponible, faites-le manuellement :

1. Connectez-vous au périphérique actif et au périphérique en veille et consultez les listes des tâches. Attendez que toutes les tâches aient fini de s'exécuter sur les deux périphériques. Si vous remettez la haute disponibilité trop tôt, vous pourriez avoir un problème futur dans lequel le basculement provoque une panne.
2. Sélectionnez **Périphérique** > **Haute disponibilité**, puis **Reprendre** la haute disponibilité dans le menu engrenage ( ).

Le basculement ne se produit pas avec une paire de versions mixtes.

Bien que l'avantage de la haute disponibilité soit que vous puissiez mettre à niveau votre déploiement sans interruption de trafic ni inspection, le basculement est désactivé pendant l'ensemble du processus de mise à niveau. C'est-à-dire que non seulement le basculement est nécessairement désactivé lorsqu'un périphérique est hors ligne (car il n'y a rien vers lequel le basculement est effectué), mais le basculement est également désactivé avec les paires de versions mixtes. C'est le seul moment où les paires de versions mixtes sont autorisées (temporairement) pendant la mise à niveau. Planifiez les mises à niveau pendant les périodes de maintenance, au moment où elles auront le moins d'incidence en cas de problème, et assurez-vous d'avoir suffisamment de temps pour mettre à niveau les deux périphériques dans cette fenêtre.

Échec de la mise à niveau sur un seul périphérique, ou un périphérique a été annulé. La paire utilise maintenant des versions mixtes.

Les paires de versions ne sont pas prises en charge pour les opérations générales. Mettez à niveau le périphérique de version antérieure ou inversez le périphérique de version ultérieure. Pour les correctifs, car la restauration n'est pas prise en charge, si vous ne pouvez pas mettre à niveau le périphérique de version antérieure, vous devez interrompre la haute disponibilité, recréer l'image d'un ou des deux périphériques, puis rétablir la haute disponibilité.

Remplacement d'une unité dans une paire à haute disponibilité

Au besoin, vous pouvez remplacer une unité dans un groupe à haute disponibilité sans perturber le trafic réseau.

Procédure

Étape 1 Si l'unité que vous remplacez est fonctionnelle, assurez-vous de basculer vers l'unité homologue, puis utilisez la commande **shutdown** à partir de l'interface de ligne de commande du périphérique pour le mettre hors service correctement. Si l'unité n'est pas fonctionnelle, confirmez que l'homologue fonctionne en mode actif.

Si vous disposez de privilèges d'administrateur, vous pouvez également entrer la commande **shutdown** par le biais de la console d'interface de ligne de commande Gestionnaire de périphériques de pare-feu.

Étape 2 Retirez l'unité du réseau.

Étape 3 Installez l'unité de remplacement et reconnectez les interfaces.

Étape 4 Terminez l'assistant de configuration du périphérique sur l'unité de remplacement.

Étape 5 Sur l'unité homologue, accédez à la page High Availability (Haute disponibilité) et copiez la configuration dans le presse-papiers. Notez s'il s'agit de l'unité principale ou secondaire.

Si des modifications sont en attente, déployez-les et attendez la fin du déploiement.

Étape 6 Sur l'unité de remplacement, cliquez sur **Configure** (Configurer) dans le groupe **High Availability** (Haute disponibilité), puis sélectionnez le type d'unité opposé parmi l'homologue. Autrement dit, si l'homologue est principal, sélectionnez **Secondary** (Secondaire), si l'homologue est secondaire, sélectionnez **Primary** (Primaire).

Étape 7 Collez la configuration de haute disponibilité de l'homologue, puis saisissez la clé IPsec si vous en utilisez une. Cliquez sur **Activate HA** (Activer HA).

Une fois le déploiement terminé, l'unité communiquera avec l'homologue et rejoindra le groupe de haute disponibilité. La configuration de l'homologue actif sera importée et l'unité de remplacement sera l'unité principale ou secondaire du groupe, en fonction de votre sélection. Vous pouvez maintenant vérifier que la haute disponibilité fonctionne correctement et, si vous le souhaitez, changer de mode pour que la nouvelle unité soit l'unité active.

Surveillance de la haute disponibilité

Les rubriques suivantes expliquent comment surveiller la haute disponibilité.

Notez que Event Viewer (Visionneuse d'événements) et les tableaux de bord affichent uniquement les données liées à l'appareil auquel vous êtes connecté. Ils n'affichent pas les données fusionnées des deux appareils.

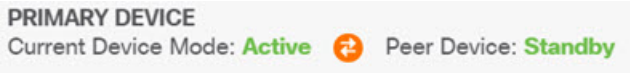
Surveillance de l'état et de l'historique du basculement général

Vous pouvez surveiller l'état général et l'historique de haute disponibilité à l'aide des éléments suivants :

- Dans Device Summary (Résumé du périphérique) (cliquez sur **Device** (Périphérique)), le groupe High Availability (Haute disponibilité) affiche l'état de l'unité.



- Sur la page High Availability (Haute disponibilité) (cliquez sur **Device (Périphérique)** > **High Availability (Haute disponibilité)**), vous pouvez voir l'état des deux unités. Si des défaillances se sont produites, la dernière raison de défaillance (provenant de l'historique de basculement) s'affiche. Cliquez sur l'icône de synchronisation entre eux pour obtenir un état supplémentaire.



- Dans la page High Availability (Haute disponibilité), cliquez sur le lien **Failover History** (Historique de basculement) à côté de l'état. Le système ouvre la console CLI et exécute la commande **show failover history details**. Vous pouvez également entrer cette commande directement dans la CLI ou la console CLI.

Commandes de l'interface de ligne de commande

À partir de la CLI ou de la console CLI, vous pouvez utiliser les commandes suivantes :

- **show failover**

  Affiche des informations sur l'état de basculement de l'unité.

- **show failover history** [**details**]

  Affiche les changements d'état de basculement passés et la raison du changement d'état. Ajoutez le mot-clé **details** pour afficher l'historique de basculement à partir de l'unité homologue. Ces renseignements aident au dépannage.

- **show failover state**

  Affiche l'état de basculement des deux unités. Les informations affichées comprennent l'état principal ou secondaire de l'unité, l'état actif ou en veille de l'unité et le dernier motif signalé pour le basculement.

- **show failover statistics**

  Affiche le nombre de paquets de transmission (tx) et de réception (rx) de l'interface de basculement. Par exemple, si la sortie indique que l'unité envoie des paquets, mais n'en reçoit aucun, vous avez un problème de liaison. Il peut s'agir d'un mauvais câble, de mauvaises adresses IP configurées sur les homologues ou encore du fait que les unités connectent les interfaces de basculement à des sous-réseaux différents.

```
> show failover statistics
        tx:320875
        rx:0
```

- **show failover interface**

  Affiche la configuration des liens de basculement et de basculement avec état. Par exemple :

```
> show failover interface
        interface failover-link GigabitEthernet1/3
                System IP Address: 192.168.10.1 255.255.255.0
                My IP Address    : 192.168.10.1
                Other IP Address : 192.168.10.2
        interface stateful-failover-link GigabitEthernet1/4
                System IP Address: 192.168.11.1 255.255.255.0
                My IP Address    : 192.168.11.1
                Other IP Address : 192.168.11.2
```

- **show monitor-interface**

  Affiche les renseignements sur les interfaces surveillées pour la haute disponibilité. Pour de plus amples renseignements, consultez la section Surveillance de l'état pour les interfaces surveillées par la haute disponibilité, à la page 243.

- **show running-config failover**

  Affiche les commandes de basculement dans la configuration actuelle. Ce sont les commandes qui configurent la haute disponibilité.

Surveillance de l'état pour les interfaces surveillées par la haute disponibilité

Si vous avez activé la surveillance HA pour toute interface, vous pouvez vérifier l'état des interfaces surveillées dans la CLI ou la console CLI à l'aide de la commande **show monitor-interface**.

```
> show monitor-interface
 This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
 Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```

Les interfaces surveillées peuvent avoir l'état suivant :

- (En attente) associé à tout autre état, comme Inconnu (En attente) — l'interface n'a pas encore reçu de paquet Hello de l'interface correspondante sur l'unité homologue.
- Inconnu : état initial. Cet état peut également signifier qu'il ne peut pas être déterminé.
- Normal : l'interface reçoit du trafic.
- En test : les messages Hello ne sont pas entendus sur l'interface pendant cinq cycles d'interrogation.
- Liaison en panne : l'interface ou le VLAN est administrativement inactif.
- Aucune liaison : le lien physique de l'interface est inactif.
- Échec : aucun trafic n'est reçu sur l'interface, mais le trafic est diffusé sur l'interface homologue.

Surveillance des messages Syslog liés à la haute disponibilité

Le système envoie un certain nombre de messages de journal système liés au basculement au niveau de priorité 2, ce qui indique une condition critique. 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. Pour obtenir une explication des messages syslog, consultez le guide *Messages syslog de Cisco Firepower Threat Defense* à l'adresse https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html.



Remarque Lors du basculement, le système s'éteint logiquement, puis affiche les interfaces, générant les messages syslog 411001 et 411002. Il s'agit d'une activité normale.

Pour pouvoir voir les messages du journal système, vous devez configurer la journalisation des diagnostics dans **Device (Périphérique)** > **Logging Settings (Paramètres de journalisation)**. Configurez un serveur syslog externe afin de pouvoir surveiller les messages de manière fiable.

Exécution à distance des commandes CLI sur l'unité homologue

À partir de l'interface de ligne de commande, vous pouvez entrer des commandes afficher sur le périphérique homologue à l'aide de la commande exec de basculement sans avoir à vous connecter à l'homologue.

failover exec {**active** | **standby** | **mate**} *commande*

Vous devez indiquer quelle unité doit exécuter la commande, qu'elle soit active ou en veille, ou entrer **mate** si vous souhaitez vous assurer que l'autre unité répond au lieu de l'unité à laquelle vous êtes connecté.

Par exemple, si vous souhaitez voir la configuration de l'interface et les statistiques de l'unité homologue, vous pouvez saisir :

```
> failover exec mate show interface
```

Vous ne pouvez pas entrer de commandes **configure**. Cette fonctionnalité est à utiliser avec les commandes **show**.



Remarque Si vous êtes connecté à l'unité active, vous pouvez recharger l'unité de secours à l'aide de la commande **failover reload-standby**.

Vous ne pouvez pas entrer ces commandes par le biais de la console d'interface de ligne de commande Gestionnaire de périphériques de pare-feu.

Dépannage de la haute disponibilité (basculement)

Si les unités d'un groupe à haute disponibilité ne fonctionnent pas comme prévu, tenez compte des étapes suivantes pour résoudre les problèmes de configuration.

Si l'unité active affiche l'unité homologue comme échec, voir Dépannage de l'état de défaillance d'une unité, à la page 246.

Procédure

Étape 1 À partir de chaque périphérique (principal et secondaire) :

- Envoyez un message Ping à l'adresse IP de l'autre périphérique pour la liaison de basculement.
- Envoyez un message Ping à l'adresse IP de l'autre périphérique pour la liaison de basculement dynamique si vous utilisez une liaison distincte.

Si la commande Ping échoue, vérifiez que les interfaces de chaque périphérique sont connectées au même segment de réseau. Si vous utilisez une connexion directe par câble, vérifiez le câble.

Étape 2 Effectuez les vérifications générales suivantes :

- Vérifiez les adresses IP de gestion en double sur les périphériques principal et secondaire.
- Vérifiez les adresses IP de basculement en double et de basculement dynamique sur les unités.
- Vérifiez que le port d'interface équivalent sur chaque périphérique est connecté au même segment de réseau.

Étape 3 Vérifiez la liste des tâches ou le journal d'audit sur le périphérique de secours. Vous devriez voir une tâche « Importation de la configuration à partir du nœud actif » réussie après chaque déploiement réussi sur le périphérique actif. Si la tâche échoue, vérifiez la liaison de basculement et réessayez le déploiement.

Remarque
Si la liste des tâches indique qu'une tâche de déploiement a échoué, il se peut qu'il y ait eu un basculement pendant la tâche de déploiement. Si le périphérique de secours était l'unité active lorsque vous avez lancé la tâche de déploiement, mais qu'un basculement s'est produit pendant la tâche, le déploiement échouera. Pour résoudre le problème, changez de mode pour faire de l'unité de secours l'unité active, puis redéployez les modifications de configuration.

Étape 4 Utilisez la commande **show failover history** pour obtenir des informations détaillées sur les changements d'état d'un périphérique.

Certains éléments à rechercher :

- Échecs de synchronisation des applications :

```
12:41:24 UTC Dec 6 2017

App Sync     Disabled     HA state progression failed due to APP SYNC timeout
```

La phase de synchronisation d'application est l'endroit où la configuration du périphérique actif est transportée vers le périphérique de secours. Un échec de synchronisation de l'application met le périphérique à l'état désactivé, et le périphérique n'est plus disponible pour être activé.

Si le périphérique est désactivé en raison d'un problème de synchronisation d'application, vous utilisez peut-être des interfaces différentes sur les périphériques pour les points terminaux des liaisons de basculement et de basculement dynamique. Vous devez utiliser le même numéro de port pour chaque extrémité de la liaison.

Si la commande show failover (afficher le basculement) affiche le périphérique secondaire à l'état Pseudo en veille, cela peut indiquer que vous avez configuré des adresses IP différentes pour la liaison de basculement sur le périphérique secondaire de celles que vous avez configurées sur le périphérique principal. Assurez-vous d'utiliser les mêmes adresses IP principales et secondaires sur les deux périphériques pour la liaison de basculement.

L'état de pseudo-veille peut également indiquer que vous avez configuré différentes clés IPsec sur les périphériques principal et secondaire.

Pour d'autres problèmes de synchronisation d'applications, consultez Dépannage des échecs de synchronisation des applications à haute disponibilité, à la page 247.

- Des basculements anormalement fréquents (passant de « actif » à « de secours ») peuvent indiquer des problèmes de liaison de basculement. Dans le pire des cas, les deux unités peuvent devenir actives, ce qui perturbe le trafic. Envoyez un message Ping à chaque extrémité du lien pour vérifier la connectivité.

Vous pouvez également utiliser **show arp** pour vérifier que l'adresse IP de basculement et le mappage ARP sont appropriés.

Si la liaison de basculement est saine et configurée correctement, envisagez d'augmenter l'interrogation de l'homologue et le délai de rétention, l'interrogation et le temps de rétention de l'interface, de réduire le nombre d'interfaces surveillées pour la haute disponibilité ou d'augmenter le seuil d'interface.

- Défaillances dues aux vérifications de l'interface. La raison de la vérification de l'interface comprend une liste des interfaces qui ont été considérées comme ayant échoué. Vérifiez ces interfaces pour vous assurer qu'elles sont correctement configurées et qu'il n'y a aucun problème matériel. Vérifiez qu'il n'y a aucun problème de configuration du commutateur à l'autre extrémité des liaisons. S'il n'y a aucun problème, envisagez de désactiver la surveillance de haute disponibilité sur ces interfaces. Vous pouvez aussi augmenter le seuil de défaillance de l'interface ou le délai associé.

```
06:17:51 UTC Jan 15 2017

Active    Failed    Interface check

                        This Host:3

                           admin: inside

                           ctx-1: ctx1-1

                           ctx-2: ctx2-1

                        Other Host:0
```

Étape 5 Si l'unité de secours ne peut pas être détectée et que vous ne trouvez pas de raison précise, comme une mauvaise connexion de réseau local (LAN) ou de câble sur la liaison de basculement, essayez les étapes suivantes.

a) Connectez-vous à l'interface de ligne de commande sur l'unité de secours et entrez la commande **failover reset**. Cette commande devrait faire passer une unité de l'état de défaillance à un état normal. Vérifiez maintenant l'état de HA sur le périphérique actif. Si l'homologue de secours est maintenant détecté, l'opération est terminée.

b) Connectez-vous à l'interface de ligne de commande sur l'unité active et entrez la commande **failover reset**. Cela devrait réinitialiser l'état de HA sur les unités active et de secours. Idéalement, cela rétablira le lien entre les périphériques. Vérifiez l'état de HA ; s'il n'est pas encore correct, poursuivez.

c) Soit à partir de l'interface de ligne de commande sur le périphérique actif, soit à partir de Gestionnaire de périphériques de pare-feu, suspendez d'abord la haute disponibilité, puis réactivez-la. Les commandes CLI sont **configure high-availability suspend** et **configure high-availability resume**.

d) Si ces étapes échouent, **reboot** le périphérique de secours.

Dépannage de l'état de défaillance d'une unité

Si une unité est marquée comme échec dans l'état de haute accessibilité de l'unité homologue (sur la page **Device (Périphérique)** ou **Device (Périphérique)** > **(High Availability (Haute accessibilité)**), voici les raisons générales possibles en fonction de l'unité A étant l'unité active et de l'unité B étant l'homologue défaillant.

- Si l'unité B n'a pas encore été configurée pour la haute accessibilité (elle est toujours en mode Standalone (Autonome)), l'unité A l'affiche comme Failed (Échec).

- Si vous suspendez la haute accessibilité sur l'unité B, l'unité A l'affichera comme Failed (Échec).
- Si vous redémarrez l'unité B, l'unité A l'affichera comme Failed (Échec) jusqu'à ce que l'unité B termine le redémarrage et reprenne la communication sur la liaison de basculement.
- Si la synchronisation de l'application (App Sync) échoue sur l'unité B, l'unité A l'affichera comme Failed (Échec). Consultez Dépannage des échecs de synchronisation des applications à haute disponibilité, à la page 247.
- Si l'unité B échoue dans la surveillance de l'intégrité de l'unité ou de l'interface, l'unité A le marque comme ayant échoué. Vérifiez l'unité B pour détecter les problèmes système. Essayez de redémarrer le périphérique. Si l'unité présente globalement une intégrité satisfaisante, envisagez d'assouplir les paramètres de surveillance de l'intégrité de l'unité ou de l'interface. La sortie de **show failover history** devrait fournir des informations sur les échecs de contrôle d'intégrité de l'interface.
- Si les deux unités deviennent actives, chaque unité affichera l'homologue comme ayant échoué. Cela indique généralement un problème de liaison de basculement.

  Cela peut également indiquer un problème de licence. Les périphériques doivent avoir une licence cohérente, soit en mode d'évaluation, soit enregistrée. S'ils sont enregistrés, les comptes de licences Smart utilisés peuvent être différents, mais les deux comptes doivent avoir la même sélection pour les fonctionnalités contrôlées à l'exportation, qu'elles soient activées ou désactivées. Si vous configurez une clé de chiffrement IPsec avec des paramètres incohérents pour les fonctionnalités contrôlées à l'exportation, les deux appareils deviendront actifs après l'activation de la haute accessibilité. Cela aura une incidence sur le routage des segments de réseau pris en charge, et vous devrez interrompre manuellement la haute accessibilité sur l'unité secondaire pour récupérer.

Dépannage des échecs de synchronisation des applications à haute disponibilité

Si l'unité homologue ne parvient pas à rejoindre le groupe à haute disponibilité, ou si elle échoue pendant que vous déployez des modifications à partir de l'unité active, connectez-vous à l'unité défaillante, accédez à la page **High Availability** (Haute disponibilité), puis cliquez sur le lien **Failover History** (Historique de basculement). Si la sortie **show failover history** indique un échec de synchronisation d'application, il y a eu un problème pendant la phase de validation de la haute disponibilité, où le système vérifie que les unités peuvent fonctionner correctement en tant que groupe de haute disponibilité.

Ce type de défaillance peut ressembler à ce qui suit :

```
==========================================================================
From State                To State                  Reason
==========================================================================
16:19:34 UTC May 9 2018
Not Detected              Disabled                  No Error

17:08:25 UTC May 9 2018
Disabled                  Negotiation               Set by the config command

17:09:10 UTC May 9 2018
Negotiation               Cold Standby              Detected an Active mate

17:09:11 UTC May 9 2018
Cold Standby              App Sync                  Detected an Active mate

17:13:07 UTC May 9 2018
```

```
App Sync                    Disabled                    CD App Sync error is
High Availability State Link Interface Mismatch between Primary and Secondary Node
```

Idéalement, vous souhaitez voir le message « Toute la validation a été transmise » lorsque l'état de provenance est Synchronisation d'application, et le nœud atteindra l'état prêt en veille. Tout échec de validation fera passer l'homologue à l'état désactivé (échec). Vous devez résoudre les problèmes pour que les homologues fonctionnent à nouveau en tant que groupe à haute disponibilité. Notez que si vous corrigez une erreur de synchronisation d'applications en modifiant l'unité active, vous devez les déployer, puis relancer la haute disponibilité pour que le nœud homologue se joigne.

Les messages suivants indiquent les échecs, avec une explication de la façon dont vous pouvez résoudre les problèmes. Ces erreurs peuvent se produire lors de la jonction de nœuds et lors de chaque déploiement ultérieur. Lors de la jonction de nœuds, le système effectue une vérification par rapport à la dernière configuration déployée sur l'unité active.

- Incompatibilité du mode d'enregistrement de licence entre le nœud principal et le nœud secondaire.

  L'erreur de licence indique qu'un homologue est enregistré alors que l'autre homologue est en mode d'évaluation. Les homologues doivent être tous deux enregistrés ou en mode d'évaluation pour qu'ils rejoignent un groupe à haute disponibilité. Comme vous ne pouvez pas faire revenir un périphérique enregistré en mode d'évaluation, vous devez enregistrer l'autre homologue à partir de la page **Device (Périphérique)** > **Smart License (Licence Smart)**.

  Si le périphérique que vous enregistrez est l'unité active, après l'enregistrement du périphérique, effectuez un déploiement. Le déploiement force les unités à actualiser et à synchroniser les configurations, ce qui devrait permettre à l'unité secondaire de rejoindre correctement le groupe de haute disponibilité.

- Incompatibilité de conformité d'exportation de licences entre le nœud principal et le nœud secondaire.

  L'erreur de conformité de licence indique que les périphériques sont enregistrés sur différents comptes Cisco Smart Software Manager, et qu'un compte est activé pour la fonctionnalité contrôlée à l'exportation, alors que l'autre ne l'est pas. Les périphériques doivent être enregistrés avec des comptes qui ont le même paramètre, activé ou désactivé, pour la fonctionnalité contrôlée à l'exportation. Modifiez l'enregistrement du périphérique sur la page **Device (Périphérique)** > **Smart License (Licence Smart)**.

- Disparité de version logicielle entre le nœud principal et le nœud secondaire.

  L'erreur d'incompatibilité de version logicielle indique que les homologues exécutent des versions différentes du logiciel Firewall Threat Defense. Le système n'autorise une incompatibilité que temporairement, pendant que vous installez des mises à niveau logicielles, un périphérique à la fois. Cependant, vous ne pouvez pas déployer les modifications de configuration entre la mise à niveau des homologues. Pour résoudre ce problème, mettez à niveau l'homologue, puis reprenez le déploiement.

- Incompatibilité des interfaces physiques entre le nœud principal et le nœud secondaire.

  L'unité de secours dans un groupe à haute disponibilité doit avoir toutes les interfaces physiques qui existent sur l'unité active, et ces interfaces doivent avoir les mêmes noms de matériel et les mêmes types (comme GigabitEthernet1/1). Cette erreur indique qu'il manque dans l'unité de secours certaines interfaces présentes dans l'unité active. Vous êtes autorisé à avoir plus d'interfaces sur l'unité de secours que sur l'unité active ; vous pouvez donc soit permuter l'unité active, soit choisir une autre unité homologue. Cependant, une incompatibilité d'interfaces ne devrait être que temporaire, par exemple si vous remplacez un module d'interface sur une unité et que vous devez la faire fonctionner sans ce module pendant une courte période. Pour le fonctionnement normal, les deux unités doivent avoir le même nombre et les mêmes types d'interfaces.

- Incompatibilité d'interface de liaison de basculement entre le nœud principal et le nœud secondaire.

Lorsque vous liez l'interface physique de basculement au réseau sur chaque unité, vous devez choisir la même interface physique. Par exemple, GigabitEthernet1/8 sur chaque unité. Cette erreur indique que vous avez utilisé des interfaces différentes. Pour résoudre l'erreur, corrigez le câblage sur l'unité homologue.

- Incompatibilité d'interface de liaison de basculement dynamique entre le nœud principal et le nœud secondaire.

  Si vous utilisez une liaison de basculement dynamique distincte, lorsque vous liez l'interface physique de basculement dynamique au réseau sur chaque unité, vous devez choisir la même interface physique. Par exemple, GigabitEthernet1/7 sur chaque unité. Cette erreur indique que vous avez utilisé des interfaces différentes. Pour résoudre l'erreur, corrigez le câblage sur l'unité homologue.

- Incompatibilité des interfaces membres d'EtherChannel du lien de basculement/de basculement dynamique entre le nœud principal et le nœud secondaire

  Si vous sélectionnez une interface EtherChannel pour les interfaces de basculement ou de basculement dynamique, les EtherChannels doivent avoir le même ID et les mêmes interfaces membres sur chaque périphérique. Ce message d'erreur indique s'il s'agit du basculement ou de la liaison de basculement dynamique qui présente l'incompatibilité. Pour résoudre l'erreur, corrigez la configuration des interfaces EtherChannel de manière à ce qu'elles utilisent le même ID et incluent les mêmes interfaces sur chaque périphérique.

- Disparité du numéro de modèle du périphérique entre le nœud principal et le nœud secondaire.

  Pour que les homologues rejoignent un groupe à haute disponibilité, ils doivent être des périphériques exactement du même modèle. Cette erreur indique que les homologues ne sont pas du même modèle de périphérique. Vous devez choisir un autre homologue pour configurer la haute disponibilité.

- Les nœuds actifs et de secours ne peuvent pas se trouver sur le même châssis.

  Vous ne pouvez pas configurer la haute disponibilité à l'aide de périphériques hébergés sur le même châssis matériel. Lors de la configuration de la haute disponibilité sur des modèles qui prennent en charge plusieurs périphériques sur le même châssis, vous devez sélectionner des périphériques qui résident sur du matériel distinct.

- Une erreur inconnue s'est produite, veuillez réessayer.

  Une erreur s'est produite lors de la synchronisation de l'application, mais le système n'a pas pu identifier le problème. Essayez de déployer la configuration à nouveau.

- Le paquet de règles est corrompu. Veuillez mettre à jour le paquet de règles et réessayer.

  Il y a un problème avec la base de données des règles de prévention des intrusions. Sur l'homologue défaillant, accédez à **Device (Périphérique)** > **Updates (Mises à jour)**, puis cliquez sur **Update Now (Mettre à jour maintenant)** dans le groupe **Rule (Règle)**. Attendez que la mise à jour soit terminée et déployez les modifications. Vous pouvez ensuite réessayer le déploiement à partir de l'unité active.

- Incompatibilité de l'état d'inscription du service en nuage entre le nœud principal et le nœud secondaire.

  L'un des nœuds est inscrit au nuage Cisco, mais l'autre n'est pas inscrit. Les deux nœuds doivent être inscrits ou aucun ne peut être inscrit pour former un groupe à haute disponibilité. Accédez à **Device (Périphérique)** > **System Settings (Paramètres du système)** > **Cloud Services (Services en nuage)** sur chacun des périphériques et assurez-vous que les deux périphériques sont inscrits dans la même région Cloud Services.

- Les nœuds Actif et de secours ne peuvent pas avoir de régions de nuage différentes.

Les appareils sont enregistrés dans différentes régions de services en nuage Cisco. Déterminez quelle région est correcte, annulez l'enregistrement de l'autre périphérique des licences Smart et sélectionnez la région correcte lors du réenregistrement. Si les deux périphériques ont la mauvaise région, annulez l'enregistrement des deux périphériques et réenregistrez-les dans la bonne région.

- Le paquet de déploiement est corrompu. Veuillez réessayer.

  Il s'agit d'une erreur de système interne. Réessayez le déploiement, ce qui devrait résoudre le problème.



CHAPITRE 11

Interfaces

Les rubriques suivantes expliquent comment configurer les interfaces sur votre appareil Firepower Threat Defense.

- À propos des interfaces Firewall Threat Defense, à la page 251
- Lignes directrices et limites des interfaces, à la page 255
- Configurer une interface physique, à la page 256
- Configurer des groupes de ponts, à la page 261
- Configurer les EtherChannels, à la page 265
- Configurer les interfaces VLAN et les ports de commutation, à la page 276
- Configurer les sous-interfaces VLAN et la jonction 802.1Q, à la page 289
- Configurer des interfaces passives, à la page 294
- Configurer les options d'interface avancées, à la page 298
- Analyser les modifications d'interface et migrer une interface, à la page 302
- Configurer le contournement matériel automatique en cas de panne de courant (ISA 3000), à la page 307
- Surveillance des interfaces, à la page 310
- Exemples d'interfaces, à la page 311

À propos des interfaces Firewall Threat Defense

Firewall Threat Defense comprend des interfaces de données ainsi qu'une interface Management (gestion)/Diagnostic.

Lorsque vous connectez un câble à un point de connexion d'interface (physiquement ou virtuellement), vous devez configurer l'interface. Au minimum, vous devez nommer l'interface et l'activer pour qu'elle puisse faire passer le trafic. Si l'interface est membre d'un groupe de ponts, il suffit de nommer l'interface. Pour les non-membres du groupe de ponts, vous devez également attribuer une adresse IP à l'interface. Si vous avez l'intention de créer des sous-interfaces VLAN plutôt qu'une interface physique unique sur un port donné, vous devez généralement configurer les adresses IP sur la sous-interface, et non sur l'interface physique. Les sous-interfaces VLAN permettent de diviser une interface physique en plusieurs interfaces logiques étiquetées avec différents ID de VLAN, ce qui est utile lorsque vous vous connectez à un port de jonction sur un commutateur. Vous ne configurez pas d'adresses IP sur les interfaces passives.

La page **Interfaces** comprend des sous-pages pour les types d'interfaces : **Interfaces** (pour les interfaces physiques), **Bridge Groups (Groupes de ponts)**, **Virtual Tunnel Interfaces (Interfaces de tunnel virtuel)**, **EtherChannels** et **VLANs** (pour le Firepower 1010 et). Notez que les EtherChannels Firepower 4100/9300 sont répertoriés sur la page **Interfaces** et non sur la page **EtherChannel**, car vous ne pouvez modifier les

paramètres EtherChannel que dans FXOS, et non dans le Gestionnaire de périphériques de pare-feu. Chaque page affiche les interfaces disponibles : leurs noms, adresses, modes et états. Vous pouvez modifier l'état d'une interface, activée ou désactivée, directement dans la liste des interfaces. La liste affiche les caractéristiques de l'interface en fonction de votre configuration. Utilisez la flèche d'ouverture/fermeture sur une interface de groupe de ponts, EtherChannel ou VLAN pour afficher les interfaces membres, qui apparaissent également d'elles-mêmes dans la liste appropriée. Vous pouvez également afficher les sous-interfaces pour les interfaces parentes prises en charge.

Les rubriques suivantes expliquent les limites de la configuration des interfaces au moyen de Gestionnaire de périphériques de pare-feu ainsi que d'autres concepts de gestion des interfaces.

Modes d'interface

Vous pouvez configurer l'un des modes suivants pour chaque interface :

Acheminé

Chaque interface routée de couche 3 nécessite une adresse IP sur un sous-réseau unique. Vous attachez généralement ces interfaces à des commutateurs, à un port d'un autre routeur ou à une passerelle de fournisseur de services Internet/de réseau étendu (WAN).

Passif

Les interfaces passives surveillent le trafic circulant sur un réseau à l'aide d'un commutateur SPAN ou d'un port miroir. Le port SPAN ou miroir permet de copier le trafic d'autres ports du commutateur. Cette fonction assure la visibilité du système dans le réseau sans être dans le flux du trafic réseau. Lorsqu'il est configuré dans un déploiement passif, le système ne peut pas prendre certaines mesures telles que le blocage ou la mise en forme du trafic. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis.

Ports de commutation (Firepower 1010)

Les ports de commutation redirigent le trafic au niveau de la couche 2 en utilisant la fonction de commutation matérielle. 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 Firepower Threat Defense. 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. Vous ne pouvez pas configurer l'interface de gestion comme port de commutation.

Membre du groupe du pont

Un groupe de ponts est un groupe d'interfaces que le périphérique Firepower Threat Defense relie par des ponts au lieu de routes. 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 pont.

Vous pouvez acheminer entre les interfaces routées et les BVI, si vous nommez le BVI. Dans ce cas, le BVI agit comme passerelle entre les interfaces membres et les interfaces routées. Si vous ne nommez pas le BVI, le trafic sur les interfaces de membre du groupe de ponts ne peut pas quitter le groupe de ponts. Normalement, vous devez nommer l'interface afin de pouvoir acheminer les interfaces membres vers Internet.

L'une des utilisations d'un groupe de ponts en mode routé consiste à utiliser des interfaces supplémentaires sur le périphérique Firepower Threat Defense plutôt qu'un commutateur externe. Vous pouvez associer des points terminaux directement aux interfaces des membres du groupe de ponts. Vous pouvez également connecter des commutateurs pour ajouter d'autres points terminaux au même réseau que la BVI.

Interface de gestion/dépistage

Le port physique étiqueté Management (gestion) (ou pour FTDv ,l'interface virtuelle de management 0/0 (gestion 0/0)) est en fait associé à deux interfaces distinctes.

- Interface virtuelle de gestion : cette adresse IP est utilisée pour la communication du système. Il s'agit de l'adresse utilisée par le système pour les licences Smart et pour récupérer les mises à niveau de la base de données. Vous pouvez ouvrir des sessions de gestion (Gestionnaire de périphériques de pare-feu et interface de ligne de commande). Vous devez configurer une adresse de gestion, qui est définie sur **System Settings (paramètres système)** > **Management Interface (interface de gestion)**.
- Interface virtuelle de diagnostic : vous pouvez utiliser cette interface pour envoyer des messages syslog à un serveur syslog externe. La configuration d'une adresse IP pour l'interface de diagnostic est facultative. La principale raison de configurer l'interface est de l'utiliser pour les messages syslog. Cette interface apparaît et peut être configurée sur la page **Device (appareil)** > **Interfaces**. L'interface de diagnostic autorise uniquement le trafic de gestion et n'autorise pas le trafic de transit.

(Périphériques matériels.) Une façon de configurer la gestion et le diagnostic consiste à ne pas câbler le port physique à un réseau. À la place, configurez uniquement l'adresse IP de gestion et configurez-la pour utiliser les interfaces de données comme passerelle pour obtenir les mises à jour à partir d'Internet. Ensuite, ouvrez les interfaces internes au trafic HTTPS/SSH (par défaut, HTTPS est activé) et ouvrez le Gestionnaire de périphériques de pare-feu à l'aide de l'adresse IP interne (voir Configuration de la liste d'accès de gestion, à la page 786).

Pour le FTDv, la configuration recommandée consiste à associer Management 0/0 (gestion 0/0) au même réseau que l'interface interne et à utiliser l'interface interne comme passerelle. Ne configurez pas d'adresse distincte pour le diagnostic.

Recommandations pour la configuration d'un réseau de gestion distinct

(Périphériques matériels.) Si vous souhaitez utiliser un réseau de gestion distinct, câblez l'interface de gestion physique à un commutateur ou à un routeur.

Pour Firewall Threat Defense Virtual, associez Management0/0 à un réseau distinct de celui des interfaces de données. Si vous utilisez toujours les adresses IP par défaut, vous devrez modifier l'adresse IP de gestion ou l'adresse IP de l'interface interne, car elles se trouvent sur le même sous-réseau.

Ensuite, configurez les éléments suivants :

- Sélectionnez **Device (Périphérique)** > **System Settings (Paramètres système)** > **Management Interface (Interface de gestion)** et configurez des adresses IPv4 ou IPv6 (ou les deux) sur le réseau connecté. Si vous le souhaitez, vous pouvez configurer un serveur DHCP pour fournir des adresses IPv4 à d'autres points terminaux du réseau. S'il y a un routeur avec une voie de routage vers l'Internet sur le réseau de gestion, utilisez-le comme passerelle. Sinon, utilisez les interfaces de données comme passerelle.
- Configurez une adresse pour l'interface de diagnostic (sur **Device (Périphérique)** > **Interfaces**) uniquement si vous avez l'intention d'envoyer des messages syslog vers un serveur syslog via cette interface. Sinon, ne configurez pas d'adresse pour le diagnostic; elle n'est pas nécessaire. Toute adresse IP que vous configurez doit se trouver sur le même sous-réseau que l'adresse IP de gestion et ne peut pas se trouver dans l'ensemble de serveurs DHCP. Par exemple, si vous utilisez 192.168.45.45 comme adresse de gestion et 192.168.45.46-192.168.45.254 comme ensemble DHCP, vous pouvez configurer le diagnostic en utilisant n'importe quelle adresse comprise entre 192.168.45.1 et 192.168.45.44.

Zones de sécurité

Chaque interface peut être affectée à une seule zone de sécurité. Vous appliquez votre politique de sécurité en fonction des zones. Par exemple, vous pouvez affecter l'interface interne à la zone interne; et l'interface externe avec la zone externe. Ensuite, vous pouvez configurer votre politique de contrôle d'accès pour permettre au trafic d'être acheminé de l'intérieur vers l'extérieur, mais pas de l'extérieur vers l'intérieur, par exemple.

Chaque zone a un mode qui est directement lié au mode d'interface. Vous pouvez ajouter des interfaces au même mode de zone de sécurité uniquement.

Pour les groupes de ponts, vous ajoutez des interfaces membres aux zones, vous ne pouvez pas ajouter l'interface virtuelle de pont (BVI).

Vous n'incluez pas l'interface Management (gestion)/Diagnostic dans une zone. Les zones s'appliquent uniquement aux interfaces de données.

Vous pouvez créer des zones de sécurité sur la page **Objects** (Objets).

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, vous configurez l'adresse globale sur l'interface virtuelle de pont (BVI), et non sur chaque interface membre. Vous ne pouvez spécifier aucune des adresses suivantes comme adresse globale.
  - Adresses IPv6 réservées en interne : fd00::/56 (from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
  - Une adresse non spécifiée, telle que ::/128
  - L'adresse de bouclage, ::1/128
  - adresses multidiffusion, ff00::/8
  - adresses locales du lien, fe80::/10
- 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 d'adresse ou pour les fonctions de découverte de réseau telles que la résolution d'adresse et la découverte de voisin. Dans un groupe de ponts, l'activation d'IPv6 sur l'interface BVI configure automatiquement les adresses locales de lien pour chaque interface de membre du groupe de ponts. Chaque interface doit avoir sa propre adresse, car l'adresse locale de lien n'est disponible que sur un segment et est liée à l'adresse MAC de l'interface.

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. Si vous ne configurez pas d'adresse globale, vous devez configurer l'adresse locale de lien. La configuration peut s'effectuer automatiquement ou manuellement.

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.

Lignes directrices et limites des interfaces

Les rubriques suivantes traitent de certaines des limites des interfaces.

Limites de la configuration de l'interface

Lorsque vous utilisez le Gestionnaire de périphériques de pare-feu pour configurer le périphérique, il existe plusieurs limites à la configuration de l'interface. Si vous avez besoin de l'une des fonctions suivantes, vous devez utiliser le FMC pour configurer l'appareil.

- Le mode de pare-feu routé uniquement est pris en charge. Vous ne pouvez pas configurer des interfaces transparentes en mode pare-feu.
- Vous pouvez configurer des interfaces passives, mais pas les interfaces ERSPAN.
- Vous ne pouvez pas configurer les interfaces en ligne (dans un ensemble intégré) ou le mode tap en ligne pour le traitement IPS uniquement. Les interfaces en mode IPS uniquement contournent de nombreuses vérifications de pare-feu et ne prennent en charge que la politique de sécurité IPS. En comparaison, les interfaces en mode pare-feu soumettent le trafic aux fonctions de pare-feu telles que la maintenance des flux, le suivi des états de flux aux niveaux IP et TCP, la défragmentation IP et la normalisation TCP. Vous pouvez également configurer des fonctions IPS pour ce trafic en mode pare-feu en fonction de votre politique de sécurité.
- Vous ne pouvez pas configurer interfaces redondantes.
- Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis. Firepower 4100/9300Les EtherChannels apparaissent dans la page **Interfaces** Gestionnaire de périphériques de pare-feu à côté des interfaces physiques simples.
- Vous ne pouvez ajouter qu'un seul groupe de ponts.
- Firewall Threat Defense prend en charge IPv4 PPPoE sur les interfaces de distribution uniquement. PPPoE n'est pas pris en charge sur les unités à haute disponibilité.

Nombre maximal de sous-interfaces VLAN par modèle de périphérique

Le modèle de périphérique limite le nombre maximal de sous-interfaces VLAN que vous pouvez configurer. Notez que vous pouvez configurer des sous-interfaces sur les interfaces de données uniquement, vous ne pouvez pas les configurer sur l'interface de gestion.

Le tableau suivant explique les limites pour chaque modèle de périphérique.

Modèle	Sous-interfaces VLAN maximales
Firepower 1010	60
Firepower 1120	512
Firepower 1140, 1150	1024
Firepower de la série 2100	1024
Firepower 4100	1024
Firepower 9300	1024
FTDv	50
ASA 5508-X	50
ASA 5516-X	100
ISA 3000	100

Configurer une interface physique

Au minimum, vous devez activer une interface physique pour l'utiliser. Vous devez également le nommer et configurer l'adressage IP. Vous ne configureriez pas l'adressage IP si vous avez l'intention de créer des sous-interfaces VLAN, si vous configurez une interface en mode passif ou si vous avez l'intention d'ajouter l'interface à un groupe de ponts. Firepower 4100/9300 Les EtherChannels sont affichés dans les pages Gestionnaire de périphériques de pare-feu **d'interfaces** à côté des interfaces physiques simples, et cette procédure s'applique également à ces EtherChannels. Vous devez effectuer toute la configuration matérielle des canaux EtherChannels de Firepower 4100/9300dans FXOS sur le châssis.

Remarque Pour configurer les interfaces physiques comme ports de commutateur Firepower 1010, consultez Configurer les interfaces VLAN et les ports de commutation, à la page 276.

Pour configurer les interfaces physiques comme interfaces passives, consultez Configurer l'interface physique en mode passif, à la page 297.

Vous pouvez désactiver une interface pour empêcher temporairement la transmission sur le réseau connecté. Vous n'avez pas besoin de supprimer la configuration de l'interface.

Procédure

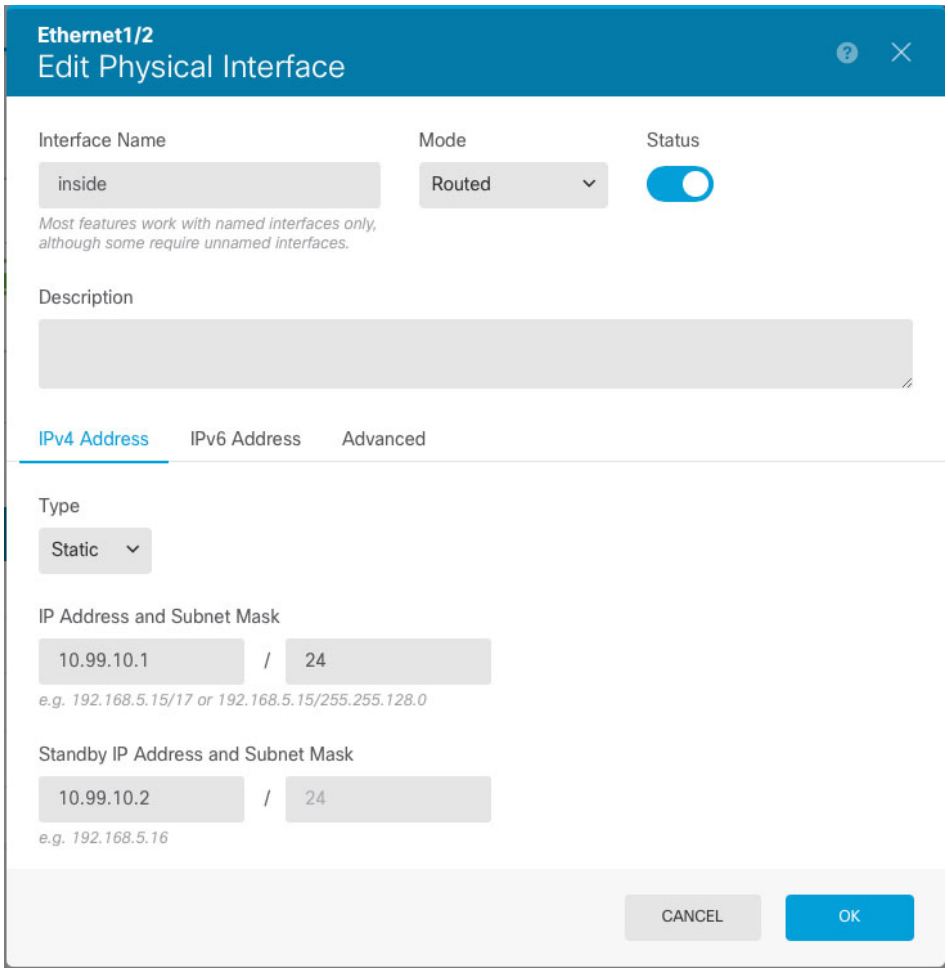
Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé des **Interfaces**.

La page **Interfaces** est sélectionnée par défaut. La liste des interfaces affiche les interfaces physiques : leurs noms, adresses et états.

Étape 2 Cliquez sur l'icône de modification ( ) pour l'interface physique que vous souhaitez modifier.

Vous ne pouvez pas modifier une interface que vous utilisez comme lien de basculement ou de basculement avec état dans une configuration à haute disponibilité.

Étape 3 Définissez les paramètres suivants :



a) Définissez le nom de l'interface (**Interface Name**).

Définissez le nom de l'interface en utilisant au maximum 48 caractères. Les caractères alphabétiques doivent être en minuscules. Par exemple, **inside** (interne) or **outside** (externe). Sans nom, le reste de la configuration de l'interface est ignoré. Sauf si vous configurez des sous-interfaces, l'interface doit avoir un nom. **Remarque :** Ne configurez pas le nom d'une interface que vous souhaitez ajouter à un canal EtherChannel.

Remarque
Si vous modifiez le nom, la modification se répercute automatiquement partout où vous avez utilisé l'ancien nom, y compris les zones de sécurité, les objets du serveur syslog et les définitions du serveur DHCP. Cependant, vous ne pouvez pas supprimer le nom avant de supprimer toutes les configurations qui utilisent le nom, car vous ne pouvez généralement pas utiliser une interface sans nom pour une politique ou un paramètre.

b) Choisissez le **Mode**.

- **Routed** (routage) : Les interfaces en mode routage soumettent le trafic aux fonctions de pare-feu telles que la maintenance des flux, le suivi des états de flux aux niveaux IP et TCP, la défragmentation IP et la normalisation TCP, ainsi que vos politiques de pare-feu. Il s'agit du mode d'interface normal.
- **Passive** (passif) : Les interfaces passives surveillent le trafic circulant sur un réseau à l'aide d'un commutateur SPAN ou d'un port miroir. Le port SPAN ou miroir permet de copier le trafic d'autres ports du commutateur. Cette fonction assure la visibilité du système dans le réseau sans être dans le flux du trafic réseau. Lorsqu'il est configuré dans un déploiement passif, le système ne peut pas prendre certaines mesures telles que le blocage ou la mise en forme du trafic. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis. Si vous sélectionnez ce mode, ne suivez pas le reste de cette procédure. Au lieu de cela, consultez Configurer l'interface physique en mode passif, à la page 297. Notez que vous ne pouvez pas configurer d'adresses IP sur les interfaces passives.
- **Switch Port** (Port de commutateur) : (Firepower 1010) Les ports de commutateur permettent la commutation matérielle entre les ports du même réseau VLAN. Le trafic commuté n'est pas soumis à la politique de sécurité. Si vous sélectionnez ce mode, ne suivez pas le reste de cette procédure. Au lieu de cela, consultez Configurer les interfaces VLAN et les ports de commutation, à la page 276.

Si vous ajoutez ultérieurement cette interface à un groupe de ponts, le mode passera automatiquement à **BridgeGroupMember** (membre du groupe de ponts). Notez que vous ne pouvez pas configurer d'adresses IP sur les interfaces des membres de groupes de ponts.

c) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

Pour les interfaces sur un Firepower 4100/9300 périphérique, vous devez également activer l'interface dans FXOS.

Si vous avez l'intention de configurer des sous-interfaces pour cette interface physique, vous avez probablement terminé. Cliquez sur **Save** (enregistrer) puis poursuivez avec Configurer les sous-interfaces VLAN et la jonction 802.1Q, à la page 289. Sinon, continuez.

Remarque
Même lors de la configuration des sous-interfaces, il est valable de nommer l'interface et de fournir les adresses IP. Ce n'est pas la configuration habituelle, mais si vous savez que c'est ce dont vous avez besoin, vous pouvez l'établir.

d) (Facultatif) Définissez la **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Étape 4 Cliquez sur l'onglet **IPv4 Address** (adresse IPv4) et configurez l'adresse IPv4.

Sélectionnez l'une des options suivantes dans le champ **Type** :

- **DHCP** : Sélectionnez cette option si l'adresse doit être obtenue du serveur DHCP sur le réseau. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Modifiez les options suivantes si nécessaire :
  - **Route Metric** (mesure de routage) : Si vous obtenez la voie de routage par défaut du serveur DHCP, il s'agit de la distance administrative par rapport à la route apprise (entre 1 et 255). La valeur par défaut est 1.
  - **Obtain Default Route** (obtenir la voie de routage par défaut) : Cette option permet d'obtenir la voie de routage par défaut à partir du serveur DHCP. Vous devez normalement sélectionner cette option, qui est la valeur par défaut.

- **Static** (statique) : Sélectionnez cette option si vous souhaitez affecter une adresse qui ne doit pas être modifiée. Saisissez l'adresse IP de l'interface et le masque de sous-réseau pour le réseau connecté à l'interface. Par exemple, si vous connectez le réseau 10.100.10.0/24, vous pouvez entrer 10.100.10.1/24. Assurez-vous que l'adresse n'est pas déjà utilisée sur le réseau.

  Si vous avez configuré la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IP de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

  Remarque
  Si un serveur DHCP est configuré pour l'interface, la configuration s'affiche. Vous pouvez modifier ou supprimer l'ensemble d'adresses DHCP. Si vous modifiez l'adresse IP de l'interface pour un sous-réseau différent, vous devez soit supprimer le serveur DHCP, soit configurer un ensemble d'adresses sur le nouveau sous-réseau, avant de pouvoir enregistrer les modifications de l'interface. Consultez Configuration du serveur DHCP, à la page 795.

- **PPPoE** : Sélectionnez cette option si l'adresse doit être obtenue à l'aide du protocole PPPoE (Point-to-point Protocol over Ethernet). PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Définissez les paramètres suivants :
  - **Group Name** (nom du groupe) : Spécifiez le nom du groupe de votre choix pour représenter cette connexion.
  - **PPPoE Username** (nom d'utilisateur PPPoE) : Spécifiez le nom d'utilisateur fourni par votre fournisseur de services Internet.
  - **PPPoE Password** : Spécifiez le mot de passe fourni par votre fournisseur de services Internet.
  - **PPP Authentication** (authentification PPP) : Choisissez **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.
  - **PPPoE Learned Route Metric** (mesure de la voie de routage apprise PPPoE) : Attribue une distance administrative à la voie de routage apprise. Cette valeur peut être comprise entre 1 et 255. Par défaut, la distance administrative pour les routes apprises est de 1.
  - **Obtain Default Route from PPPoE** (obtenir la voie de routage par défaut à partir de PPPoE) : Cochez cette case pour activer l'obtention de la voie de routage par défaut à partir du serveur PPPoE.
  - **IP Address Type (type d'adresse IP)** : Choisissez **Dynamic (dynamique)** pour obtenir l'adresse IP du serveur PPPoE. Vous pouvez également choisir **Static** (statique) si vous avez reçu une adresse IP statique du fournisseur de services Internet.

Étape 5 (Facultatif) Cliquez sur l'onglet **IPv6 Address** (adresse IPv6) et configurez l'adresse IPv6.

- **State** (état) : Pour activer le traitement IPv6 et configurer automatiquement l'adresse de liaison locale lorsque vous ne configurez pas l'adresse globale, sélectionnez **Enabled** (activé). L'adresse locale de liaison est générée en fonction des adresses MAC d'interface (format EUI-64 *modifié*).

  Remarque
  La désactivation de l'adresse IPv6 ne désactive pas le traitement IPv6 sur une interface configurée avec une adresse IPv6 explicite ou activée pour la configuration automatique.

- **Address Auto Configuration** (configuration automatique de l'adresse) : Sélectionnez cette option pour configurer l'adresse automatiquement. La configuration automatique sans état IPv6 générera une adresse IPv6 globale uniquement si le lien sur lequel le périphérique réside a un routeur configuré pour fournir des services IPv6, y compris la publicité d'un préfixe global IPv6 à utiliser sur le lien. Si les services de routage IPv6 ne sont pas disponibles sur le lien, vous obtiendrez uniquement une adresse IPv6 lien-local, à laquelle vous ne pourrez pas accéder en dehors du lien réseau immédiat de l'appareil. L'adresse locale de liaison est basée sur l'ID d'interface EUI-64 modifié.

  Bien que la RFC 4862 spécifie que les hôtes configurés pour une autoconfiguration sans état n'envoient pas de messages de publicité de routeur, le dispositif FTD envoie des messages de publicité de routeur dans ce cas. Sélectionnez **Suppress RA** (supprimer RA) pour supprimer les messages et se conformer au RFC.

- **Static Address/Prefix** (adresse statique/préfixe) : Si vous n'utilisez pas la configuration automatique sans état, saisissez l'adresse IPv6 globale statique complète et le préfixe de réseau. Par exemple : 2001:0DB8::BA98:0:3210/48. Pour en savoir plus sur l'adressage IPv6, consultez Adresse IPv6, à la page 254.

  Si vous souhaitez utiliser l'adresse comme lien local uniquement, sélectionnez l'option **Link - Local** (lien local). Les adresses locales de liaison ne sont pas accessibles en dehors du réseau local. Vous ne pouvez pas configurer une adresse lien-local sur une interface de groupe de ponts.

  Remarque
  Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. 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.

- **Standby IP Address** (adresse IP en veille) : Si vous configurez la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IPv6 de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

- **Suppress RA** : Cette option permet de supprimer les publicités de routeur. FTD peut participer à des publicités de routeur afin que les dispositifs voisins puissent apprendre de façon dynamique une adresse de routeur par défaut. Par défaut, des messages de publicité de routeur (ICMPv6 type 134) sont envoyés périodiquement à chaque interface configurée IPv6.

  Des publicités de routeur sont également envoyées en réponse à des 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 supprimer ces messages sur toute interface dont vous ne souhaitez pas que le dispositif FTD fournisse le préfixe IPv6 (par exemple, l'interface externe).

Étape 6 (Facultatif) Configurer les options avancées, à la page 300.

Les paramètres avancés comprennent des paramètres par défaut appropriés pour la plupart des réseaux. Modifiez-les uniquement lors de la résolution des problèmes de réseau.

Étape 7 Cliquez sur **OK**.

Prochaine étape

- Ajoutez les interfaces aux zones de sécurité appropriées. Consultez Configuration des zones de sécurité, à la page 148.

Configurer des groupes de ponts

Un groupe de ponts est une interface virtuelle qui regroupe une ou plusieurs interfaces. La principale raison du regroupement d'interfaces est de créer un groupe d'interfaces commutées. Ainsi, vous pouvez connecter des postes de travail ou d'autres périphériques d'extrémité directement aux interfaces incluses dans le groupe de ponts. Vous n'avez pas besoin de les connecter par l'intermédiaire d'un commutateur physique distinct, bien que vous puissiez également connecter un commutateur à un membre d'un groupe de ponts.

Les membres du groupe n'ont pas d'adresses IP. Au lieu de cela, toutes les interfaces membres partagent l'adresse IP de l'interface virtuelle de pont (BVI). Si vous activez IPv6 sur les BVI, des adresses de lien local uniques sont automatiquement attribuées aux interfaces membres.

Vous activez et désactivez les interfaces membres individuellement. Ainsi, vous pouvez désactiver toutes les interfaces inutilisées sans avoir à les supprimer du groupe de ponts. Le groupe de ponts lui-même est toujours activé.

Vous configurez généralement un serveur DHCP sur l'interface de groupe de ponts (BVI), qui fournit des adresses IP pour tous les points terminaux connectés par l'intermédiaire des interfaces membres. Cependant, vous pouvez configurer des adresses statiques sur les points terminaux connectés aux interfaces membres si vous le souhaitez. Tous les points terminaux du groupe de ponts doivent avoir des adresses IP sur le même sous-réseau que l'adresse IP du groupe de ponts.

Lignes directrices et limites relatives à la licence

- Vous ne pouvez ajouter qu'un seul groupe de ponts.
- Les EtherChannels définis par Gestionnaire de périphériques de pare-feu 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.
- Vous ne pouvez pas configurer de groupes de ponts sur Série Firepower 2100 ou les périphériques Firewall Threat Defense Virtual.
- Dans le cas du Firepower 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.
- L'ISA 3000 est préconfiguré avec le groupe de ponts BVI1 (non nommé, ce qui signifie qu'il ne participe pas au routage). BVI1 comprend toutes les interfaces de données : GigabitEthernet1/1 (outside1), GigabitEthernet1/2 (inside1), GigabitEthernet1/3 (outside2) et GigabitEthernet1/4 (inside2). Vous devez définir l'adresse IP de BVI1 pour qu'elle corresponde à votre réseau.

Avant de commencer

Configurez les interfaces qui seront membres du groupe de ponts. Plus précisément, chaque interface membre doit satisfaire aux exigences suivantes :

- L'interface doit avoir un nom.
- Aucune adresse IPv4 ou IPv6 ne peut être définie pour l'interface, qu'elle soit statique ou desservie par DHCP. Si vous devez supprimer l'adresse d'une interface que vous utilisez actuellement, vous devrez peut-être supprimer d'autres configurations pour l'interface, telles que les routes statiques, le serveur DHCP ou les règles NAT, qui dépendent du fait que l'interface possède une adresse.
- Vous devez retirer l'interface de sa zone de sécurité (si elle se trouve dans une zone) et supprimer toutes les règles NAT associées à cette interface avant de pouvoir l'ajouter à un groupe de ponts.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), cliquez sur le lien dans le résumé des **Interfaces**, puis cliquez sur **Bridge Groups** (Groupes de ponts).

La liste des groupes de ponts affiche les groupes de ponts existants. Cliquez sur la flèche d'ouverture/fermeture pour afficher les interfaces membres pour chaque groupe de ponts. Les interfaces membres s'affichent également séparément dans les pages **Interfaces** ou **VLAN**.

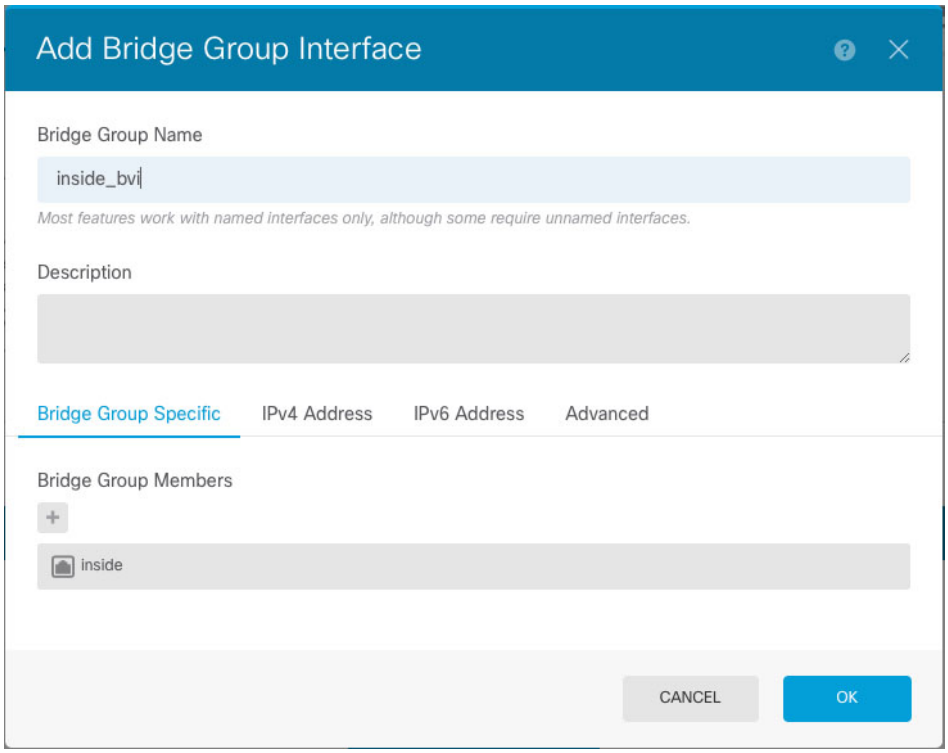
Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur l'icône de modification ( ) pour le BVI1 groupe de ponts.
- Cliquez sur **Create Bridge Grou**p (Créer un groupe de ponts) ou sur l'icône plus ( ) pour créer un nouveau groupe.

  Remarque
  Vous ne pouvez avoir qu'un seul groupe de ponts. Si vous avez déjà défini un groupe de ponts, vous devez modifier ce groupe au lieu d'essayer d'en créer un nouveau. Si vous devez créer un nouveau groupe de ponts, vous devez d'abord supprimer le groupe de ponts existant.

- Cliquez sur l'icône de suppression ( ) du groupe de ponts si vous n'en avez plus besoin. Lorsque vous supprimez un groupe de ponts, ses membres deviennent des interfaces routées standard, et toutes les règles de NAT ou l'appartenance à une zone de sécurité sont conservées. Vous pouvez modifier les interfaces pour leur attribuer des adresses IP. Si vous souhaitez les ajouter à un nouveau groupe de ponts, vous devez d'abord supprimer les règles de NAT et retirer l'interface de sa zone de sécurité.

Étape 3 Configurez les éléments suivants :



a) (Facultatif) Définissez le nom de l'interface (**Interface Name**).

Définissez le nom du groupe de ponts, en utilisant au maximum 48 caractères. Les caractères alphabétiques doivent être en minuscules. Par exemple, **inside** (interne) or **outside** (externe). Définissez le nom si vous souhaitez que ce BVI participe au routage entre lui et d'autres interfaces nommées.

Remarque
Si vous modifiez le nom, la modification se répercute automatiquement partout où vous avez utilisé l'ancien nom, y compris les zones de sécurité, les objets du serveur syslog et les définitions du serveur DHCP. Cependant, vous ne pouvez pas supprimer le nom avant de supprimer toutes les configurations qui utilisent le nom, car vous ne pouvez généralement pas utiliser une interface sans nom pour une politique ou un paramètre.

b) (Facultatif) Définissez la **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

c) Modifiez la liste des **membres du groupe de ponts**.

Vous pouvez ajouter jusqu'à 64 interfaces ou sous-interfaces à un seul groupe de ponts.

- Ajouter une interface : cliquez sur l'icône plus (+), cliquez sur une ou plusieurs interfaces, puis cliquez sur **OK**.
- Supprimer une interface : passez le curseur sur une interface et cliquez sur le **x** sur le côté droit.

Étape 4 Cliquez sur l'onglet **IPv4 Address** (adresse IPv4) et configurez l'adresse IPv4.

Sélectionnez l'une des options suivantes dans le champ **Type** :

- **Static** (statique) : Sélectionnez cette option si vous souhaitez affecter une adresse qui ne doit pas être modifiée. Saisissez l'adresse IP du groupe de ponts et le masque de sous-réseau. Tous les points d'extrémité connectés seront sur ce réseau. Assurez-vous que l'adresse n'est pas déjà utilisée sur le réseau.

  Si vous avez configuré la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IP de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

  Remarque
  Si un serveur DHCP est configuré pour l'interface, la configuration s'affiche. Vous pouvez modifier ou supprimer l'ensemble d'adresses DHCP. Si vous modifiez l'adresse IP de l'interface pour un sous-réseau différent, vous devez soit supprimer le serveur DHCP, soit configurer un ensemble d'adresses sur le nouveau sous-réseau, avant de pouvoir enregistrer les modifications de l'interface. Consultez Configuration du serveur DHCP, à la page 795.

- **Dynamic** (Dynamique) (DHCP) : sélectionnez cette option si l'adresse doit être obtenue du serveur DHCP sur le réseau. Ce n'est pas l'option habituelle pour les groupes de ponts, mais vous pouvez la configurer au besoin. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité.Modifiez les options suivantes si nécessaire :

  - **Route Metric** (mesure de routage) : Si vous obtenez la voie de routage par défaut du serveur DHCP, il s'agit de la distance administrative par rapport à la route apprise (entre 1 et 255). La valeur par défaut est 1.
  - **Obtain Default Route** (obtenir la voie de routage par défaut) : Cette option permet d'obtenir la voie de routage par défaut à partir du serveur DHCP. Vous devez normalement sélectionner cette option, qui est la valeur par défaut.

Étape 5 (Facultatif) Cliquez sur l'onglet **IPv6 Address** (adresse IPv6) et configurez l'adresse IPv6.

- **State** (état) : Pour activer le traitement IPv6 et configurer automatiquement l'adresse de liaison locale lorsque vous ne configurez pas l'adresse globale, sélectionnez **Enabled** (activé). L'adresse locale de liaison est générée en fonction des adresses MAC d'interface (format EUI-64 *modifié*).

  Remarque
  La désactivation de l'adresse IPv6 ne désactive pas le traitement IPv6 sur une interface configurée avec une adresse IPv6 explicite ou activée pour la configuration automatique.

- **Static Address/Prefix** (adresse statique/préfixe) : Si vous n'utilisez pas la configuration automatique sans état, saisissez l'adresse IPv6 globale statique complète et le préfixe de réseau. Par exemple : 2001:0DB8::BA98:0:3210/48. Pour en savoir plus sur l'adressage IPv6, consultez Adresse IPv6, à la page 254.

  Si vous souhaitez utiliser l'adresse comme lien local uniquement, sélectionnez l'option **Link - Local** (lien local). Les adresses locales de liaison ne sont pas accessibles en dehors du réseau local. Vous ne pouvez pas configurer une adresse lien-local sur une interface de groupe de ponts.

  Remarque
  Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. 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.

- **Standby IP Address** (adresse IP en veille) : Si vous configurez la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IPv6 de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.
- **Suppress RA** : Cette option permet de supprimer les publicités de routeur. Appareil FTD peut participer à des publicités de routeur afin que les dispositifs voisins puissent apprendre de façon dynamique une adresse de routeur par défaut. Par défaut, des messages de publicité de routeur (ICMPv6 type 134) sont envoyés périodiquement à chaque interface configurée IPv6.

  Des publicités de routeur sont également envoyées en réponse à des 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 supprimer ces messages sur toute interface dont vous ne souhaitez pas que le dispositif FTD fournisse le préfixe IPv6 (par exemple, l'interface externe).

Étape 6 (Facultatif) Configurer les options avancées, à la page 300.

Vous configurez la plupart des options avancées sur les interfaces *membres* de groupe de ponts, mais certaines sont disponibles pour l'interface de groupe de ponts.

Les paramètres avancés comprennent des paramètres par défaut appropriés pour la plupart des réseaux. Modifiez-les uniquement lors de la résolution des problèmes de réseau.

Étape 7 Cliquez sur **OK**.

Prochaine étape

- Assurez-vous que toutes les interfaces membres que vous avez l'intention d'utiliser sont activées.
- Configurez un serveur DHCP pour le groupe de ponts. Consultez Configuration du serveur DHCP, à la page 795.
- Ajoutez les interfaces aux zones de sécurité appropriées. Consultez Configuration des zones de sécurité, à la page 148.
- Vérifiez que les politiques, telles que l'identité, la NAT et l'accès, fournissent les services requis pour le groupe de ponts et les interfaces de membre.

Configurer les EtherChannels

Cette section décrit les EtherChannels et comment les configurer.

Remarque Vous pouvez ajouter des EtherChannels dans le champ Gestionnaire de périphériques de pare-feu aux modèles suivants :

- Firepower 1000
- Firepower de la série 2100
- ISA 3000

Vous ne pouvez pas utiliser les ports de commutation ni les interfaces VLAN de Firepower 1010 ou Cisco Secure Firewall 1210/1220 dans les EtherChannels.

Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis. Les EtherChannels Firepower 4100/9300 s'affichent dans la page Interfaces Gestionnaire de périphériques de pare-feu à côté des interfaces physiques simples. Vous ne pouvez pas non plus configurer les EtherChannels dans le Gestionnaire de périphériques de pare-feu sur d'autres modèles, comme le Firewall Threat Defense Virtual ou la série ASA 5500-X.

À propos des 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.

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.

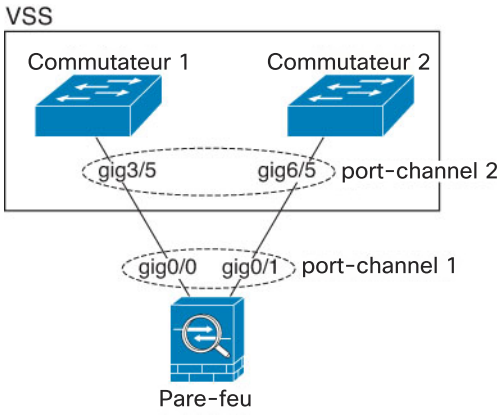
L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal. L'interface est sélectionnée à l'aide d'un algorithme de hachage exclusif, en fonction des adresses MAC source ou de destination, des adresses IP, des numéros de ports TCP et UDP et des numéros de VLAN.

Connexion à un EtherChannel sur un autre périphérique

Le périphérique auquel vous connectez l'EtherChannel FTD 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 FTD 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.

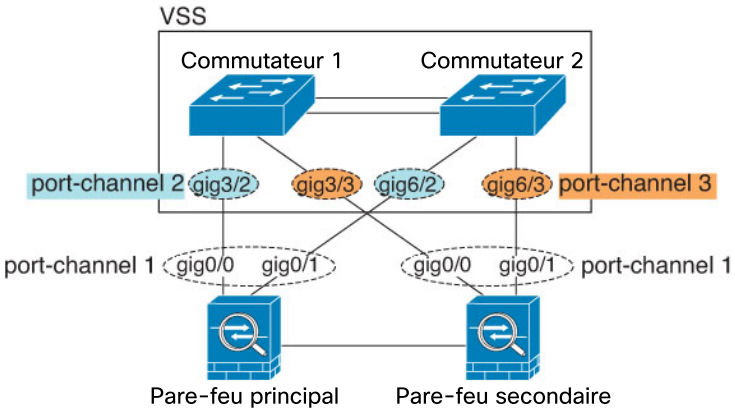
Illustration 7 : Connexion à un VSS/vPC



Remarque Si le périphérique FTD est en mode de pare-feu transparent et que vous placez le périphérique FTD 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 FTD 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 FTD dans un déploiement de basculement actif/en veille, vous devez créer des EtherChannels distincts sur les commutateurs du VSS/vPC, un pour chaque périphérique FTD. Sur chaque périphérique FTD, 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 FTD (dans ce cas, l'EtherChannel ne sera pas établi en raison des ID de système FTD distincts), un seul EtherChannel ne serait pas souhaitable, car vous ne pouvez pas souhaitez que le trafic soit envoyé au périphérique FTD.

Illustration 8 : 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.
- 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 FTD 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.

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.

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

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. 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.

Matériel ASA

L'interface de canal de port utilise l'adresse MAC d'interface de groupe de canaux de numéro le plus faible comme adresse MAC du canal de port. Vous pouvez également configurer manuellement une adresse MAC pour l'interface du canal de port. Il est recommandé de configurer manuellement, 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 faible, ce qui perturbe le trafic.

Lignes directrices pour les EtherChannels

Groupe de ponts

les EtherChannels définis par le Gestionnaire de périphériques de pare-feu ne sont pas pris en charge en tant que membres du groupe de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.

Haute disponibilité

- Lorsque vous utilisez une interface EtherChannel comme lien Haute disponibilité, elle doit être préconfigurée sur les deux unités de la paire Haute disponibilité; 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 Haute disponibilité 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 Haute disponibilité. 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 Haute disponibilité. Ce n'est que lorsque toutes les interfaces physiques tombent en panne que l'EtherChannel semble défaillante.
- Si vous utilisez une interface EtherChannel pour un Haute disponibilité 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 Haute disponibilité. Pour modifier la configuration, vous devez désactiver temporairement Haute disponibilité, ce qui empêche Haute disponibilité de se produire pendant la durée.

Prise en charge des modèles

- Vous pouvez ajouter des EtherChannels dans le champ Gestionnaire de périphériques de pare-feu aux modèles suivants :
  - Firepower 1000
  - Firepower de la série 2100
  - ISA 3000

Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis. Les EtherChannels Firepower 4100/9300 s'affichent dans la page Interfaces Gestionnaire de périphériques de pare-feu à côté des interfaces physiques simples. Vous ne pouvez pas non plus configurer les EtherChannels de Gestionnaire de périphériques de pare-feu sur d'autres modèles, comme la gamme ASA 5500-X.

- Vous ne pouvez pas utiliser les ports de commutation ni les interfaces VLAN de Firepower 1010 dans les EtherChannels.

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.
- 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. 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 FTD doit également prendre en charge l'EtherChannel 802.3ad.
- Le périphérique FTD 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 FTD abandonnera les LACPDU balisées. Assurez-vous de désactiver le balisage VLAN natif sur le commutateur voisin.
- 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 LACPest défini sur rapide par défaut dans FXOS, mais vous pouvez le configurer comme normal (également appelé lent).
  - 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, FTD 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 FTD 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 FTD fait référence à l'interface logique EtherChannel plutôt qu'aux interfaces physiques membres.

Ajouter un canal EtherChannel

Ajoutez un EtherChannel et affectez-y des interfaces membres.

Remarque Vous pouvez ajouter des EtherChannels dans le champ Gestionnaire de périphériques de pare-feu aux modèles suivants :

- Firepower 1000
- Firepower de la série 2100
- ISA 3000

Vous ne pouvez pas utiliser les ports de commutation ni les interfaces VLAN dans les EtherChannels.

Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis. Les EtherChannels Firepower 4100/9300 s'affichent dans la page Interfaces Gestionnaire de périphériques de pare-feu à côté des interfaces physiques simples. Vous ne pouvez pas non plus configurer les EtherChannels dans le Gestionnaire de périphériques de pare-feu sur d'autres modèles, comme la gamme ASA 5500-X.

Avant de commencer

- Lorsque vous ajoutez la première interface membre, elle définit les propriétés matérielles requises de toutes les interfaces membres. Consultez Lignes directrices pour les EtherChannels, à la page 269 pour plus de détails sur les exigences des interfaces membres.
- Les interfaces membres ne peuvent pas être nommées.

Mise en garde Si vous utilisez une interface déjà présente dans votre configuration, la suppression du nom effacera toute configuration faisant référence à l'interface.

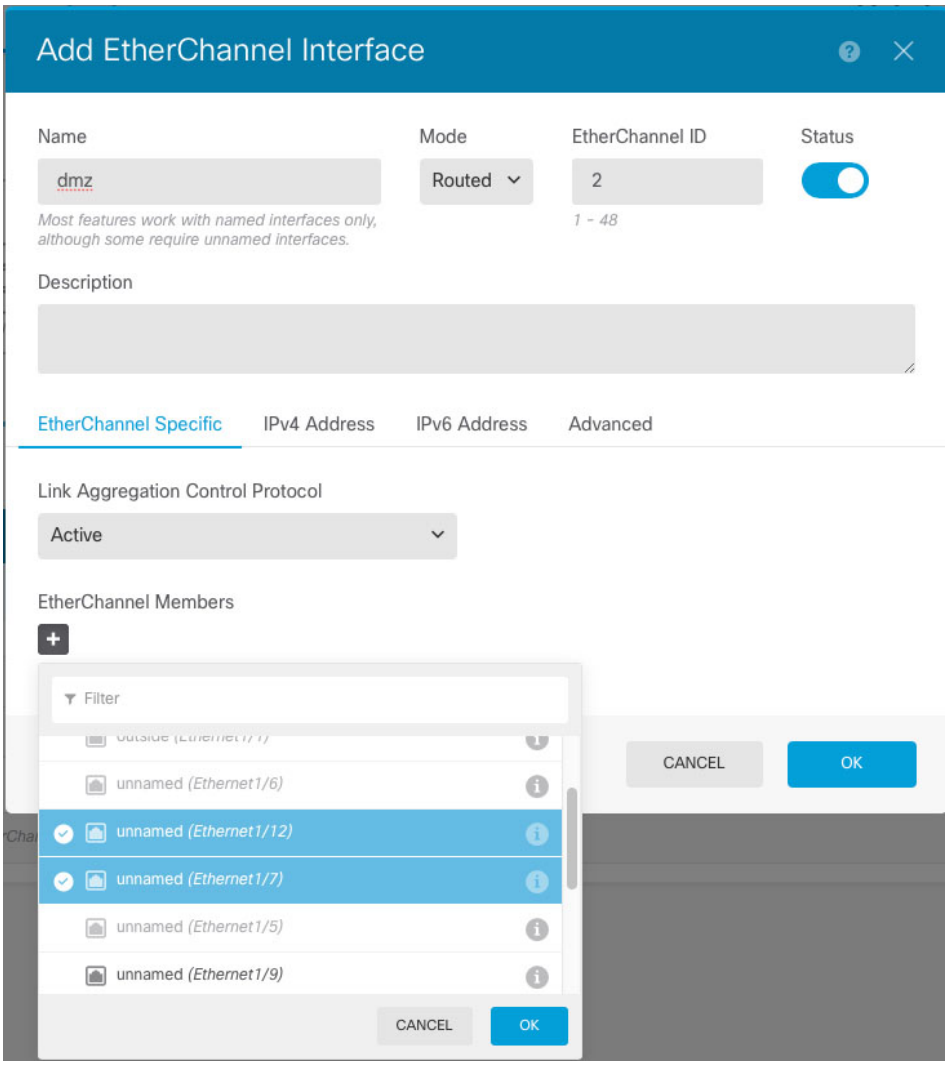
Procédure

Étape 1 Cliquez sur **Device** (périphérique), cliquez sur le lien dans le résumé **Interfaces**, puis cliquez sur **EtherChannels**.

La liste EtherChannels affiche les EtherChannels existants, leurs noms, adresses et états. Cliquez sur la flèche d'ouverture/fermeture pour afficher les interfaces membres pour chaque EtherChannel. Les interfaces membres s'affichent également séparément sur la page **Interfaces**.

Étape 2 Cliquez sur **Create EtherChannel (Créer un EtherChannel)** (s'il n'y a pas d'EtherChannel actuel) ou sur l'icône plus ( ), puis **EtherChannel** pour créer un nouvel EtherChannel.

Étape 3 Configurez les éléments suivants :



a) Définissez le nom de l'interface (**Interface Name**).

Définissez le nom de l'EtherChannel, jusqu'à 48 caractères. Les caractères alphabétiques doivent être en minuscules. Par exemple, **inside** (interne) or **outside** (externe).

Remarque
Si vous modifiez le nom, la modification se répercute automatiquement partout où vous avez utilisé l'ancien nom, y compris les zones de sécurité, les objets du serveur syslog et les définitions du serveur DHCP. Cependant, vous ne pouvez pas supprimer le nom avant de supprimer toutes les configurations qui utilisent le nom, car vous ne pouvez généralement pas utiliser une interface sans nom pour une politique ou un paramètre.

b) Définissez le **Mode**.

- **Routed** (routage) : Les interfaces en mode routage soumettent le trafic aux fonctions de pare-feu telles que la maintenance des flux, le suivi des états de flux aux niveaux IP et TCP, la défragmentation IP et la normalisation TCP, ainsi que vos politiques de pare-feu. Utilisez ce mode si vous avez l'intention de faire passer le trafic par l'interface. Il s'agit du mode d'interface normal.
- **Passive** (passif) : Les interfaces passives surveillent le trafic circulant sur un réseau à l'aide d'un commutateur SPAN ou d'un port miroir. Le port SPAN ou miroir permet de copier le trafic d'autres ports du commutateur. Cette fonction assure la visibilité du système dans le réseau sans être dans le flux du trafic réseau. Lorsqu'il est configuré dans un déploiement passif, le système ne peut pas prendre certaines mesures telles que le blocage ou la mise en forme du trafic. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis. Si vous sélectionnez ce mode, ne suivez pas le reste de cette procédure. Au lieu de cela, consultez Configurer l'interface physique en mode passif, à la page 297.

c) Définissez le **EtherChannel ID** (ID EtherChannel), entre 1 et 48 (entre 1 et 8 pour le Firepower 1010).

d) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

e) (Facultatif) Définissez la **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

f) Choisissez le **mode EtherChannel**.

- **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 ».

g) Ajoutez **les membres de l'EtherChannel**.

Vous pouvez ajouter jusqu'à 8 interfaces (sans nom) à l'EtherChannel.

- Ajouter une interface : cliquez sur l'icône plus ( ), cliquez sur une ou plusieurs interfaces, puis cliquez sur **OK**.
- Supprimer une interface : passez le curseur sur une interface et cliquez sur le **x** sur le côté droit.

Étape 4 Cliquez sur l'onglet **IPv4 Address** (adresse IPv4) et configurez l'adresse IPv4.

Sélectionnez l'une des options suivantes dans le champ **Type** :

- **DHCP** : Sélectionnez cette option si l'adresse doit être obtenue du serveur DHCP sur le réseau. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Modifiez les options suivantes si nécessaire :
  - **Route Metric** (mesure de routage) : Si vous obtenez la voie de routage par défaut du serveur DHCP, il s'agit de la distance administrative par rapport à la route apprise (entre 1 et 255). La valeur par défaut est 1.
  - **Obtain Default Route** (obtenir la voie de routage par défaut) : Cette option permet d'obtenir la voie de routage par défaut à partir du serveur DHCP. Vous devez normalement sélectionner cette option, qui est la valeur par défaut.

- **Static** (statique) : Sélectionnez cette option si vous souhaitez affecter une adresse qui ne doit pas être modifiée. Saisissez l'adresse IP de l'interface et le masque de sous-réseau pour le réseau connecté à l'interface. Par exemple, si vous connectez le réseau 10.100.10.0/24, vous pouvez entrer 10.100.10.1/24. Assurez-vous que l'adresse n'est pas déjà utilisée sur le réseau.

  Si vous avez configuré la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IP de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

  Remarque
  Si un serveur DHCP est configuré pour l'interface, la configuration s'affiche. Vous pouvez modifier ou supprimer l'ensemble d'adresses DHCP. Si vous modifiez l'adresse IP de l'interface pour un sous-réseau différent, vous devez soit supprimer le serveur DHCP, soit configurer un ensemble d'adresses sur le nouveau sous-réseau, avant de pouvoir enregistrer les modifications de l'interface. Consultez Configuration du serveur DHCP, à la page 795.

- **PPPoE** : Sélectionnez cette option si l'adresse doit être obtenue à l'aide du protocole PPPoE (Point-to-point Protocol over Ethernet). PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Définissez les paramètres suivants :

  - **Group Name** (nom du groupe) : Spécifiez le nom du groupe de votre choix pour représenter cette connexion.
  - **PPPoE Username** (nom d'utilisateur PPPoE) : Spécifiez le nom d'utilisateur fourni par votre fournisseur de services Internet.
  - **PPPoE Password** : Spécifiez le mot de passe fourni par votre fournisseur de services Internet.
  - **PPP Authentication** (authentification PPP) : Choisissez **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.
  - **PPPoE Learned Route Metric** (mesure de la voie de routage apprise PPPoE) : Attribue une distance administrative à la voie de routage apprise. Cette valeur peut être comprise entre 1 et 255. Par défaut, la distance administrative pour les routes apprises est de 1.
  - **Obtain Default Route from PPPoE** (obtenir la voie de routage par défaut à partir de PPPoE) : Cochez cette case pour activer l'obtention de la voie de routage par défaut à partir du serveur PPPoE.
  - **IP Address Type (type d'adresse IP)** : Choisissez **Dynamic (dynamique)** pour obtenir l'adresse IP du serveur PPPoE. Vous pouvez également choisir **Static** (statique) si vous avez reçu une adresse IP statique du fournisseur de services Internet.

Étape 5 (Facultatif) Cliquez sur l'onglet **IPv6 Address** (adresse IPv6) et configurez l'adresse IPv6.

- **State** (état) : Pour activer le traitement IPv6 et configurer automatiquement l'adresse de liaison locale lorsque vous ne configurez pas l'adresse globale, sélectionnez **Enabled** (activé). L'adresse locale de liaison est générée en fonction des adresses MAC d'interface (format EUI-64 *modifié*).

  Remarque
  La désactivation de l'adresse IPv6 ne désactive pas le traitement IPv6 sur une interface configurée avec une adresse IPv6 explicite ou activée pour la configuration automatique.

- **Address Auto Configuration** (configuration automatique de l'adresse) : Sélectionnez cette option pour configurer l'adresse automatiquement. La configuration automatique sans état IPv6 générera une adresse IPv6 globale uniquement si le lien sur lequel le périphérique réside a un routeur configuré pour fournir des services IPv6, y compris la publicité d'un préfixe global IPv6 à utiliser sur le lien. Si les services de routage IPv6 ne sont pas disponibles sur le lien, vous obtiendrez uniquement une adresse IPv6 lien-local, à laquelle vous ne pourrez pas accéder en dehors du lien réseau immédiat de l'appareil. L'adresse locale de liaison est basée sur l'ID d'interface EUI-64 modifié.

  Bien que la RFC 4862 spécifie que les hôtes configurés pour une autoconfiguration sans état n'envoient pas de messages de publicité de routeur, le dispositif FTD envoie des messages de publicité de routeur dans ce cas. Sélectionnez **Suppress RA** (supprimer RA) pour supprimer les messages et se conformer au RFC.

- **Static Address/Prefix** (adresse statique/préfixe) : Si vous n'utilisez pas la configuration automatique sans état, saisissez l'adresse IPv6 globale statique complète et le préfixe de réseau. Par exemple : 2001:0DB8::BA98:0:3210/48. Pour en savoir plus sur l'adressage IPv6, consultez Adresse IPv6, à la page 254.

  Si vous souhaitez utiliser l'adresse comme lien local uniquement, sélectionnez l'option **Link - Local** (lien local). Les adresses locales de liaison ne sont pas accessibles en dehors du réseau local. Vous ne pouvez pas configurer une adresse lien-local sur une interface de groupe de ponts.

  Remarque
  Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. 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.

- **Standby IP Address** (adresse IP en veille) : Si vous configurez la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IPv6 de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

- **Suppress RA** : Cette option permet de supprimer les publicités de routeur. FTD peut participer à des publicités de routeur afin que les dispositifs voisins puissent apprendre de façon dynamique une adresse de routeur par défaut. Par défaut, des messages de publicité de routeur (ICMPv6 type 134) sont envoyés périodiquement à chaque interface configurée IPv6.

  Des publicités de routeur sont également envoyées en réponse à des 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 supprimer ces messages sur toute interface dont vous ne souhaitez pas que le dispositif FTD fournisse le préfixe IPv6 (par exemple, l'interface externe).

Étape 6 Définissez la vitesse des interfaces membres en cliquant sur **Advanced (Avancé)**, et définissez la vitesse.

Vous pouvez également configurer d'autres options avancées. Consultez Configurer les options avancées, à la page 300

Étape 7 Cliquez sur **OK**.

Prochaine étape

- Ajoutez les EtherChannels aux zones de sécurité appropriées. Consultez Configuration des zones de sécurité, à la page 148.

Configurer les interfaces VLAN et les ports de commutation

Pour les modèles avec commutateur interne, vous pouvez configurer chaque interface pour qu'elle fonctionne comme une interface de pare-feu normale ou comme un port de commutateur matériel de couche 2. Cette section 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. Cette section décrit également comment personnaliser l'alimentation par Ethernet (PoE) sur les interfaces prises en charge.

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 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. Vous pouvez également configurer ces interfaces pour qu'elles soient IPS uniquement (ensembles en ligne).
- 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 FTD. 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 interfacesIPS seulement (ensembles en ligne et interfaces passives) ou des interfaces EtherChannel. Lorsqu'un port de commutation doit communiquer avec un autre réseau, le périphérique

FTD 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 FTD. 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.

Préalables pour les ports de commutation

Prise en charge des modèles

- Firepower 1010

Lignes directrices relatives aux ports de commutation

Haute disponibilité

- Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l'utilisation de Haute disponibilité. 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. Haute disponibilité 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 Haute disponibilité 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 Haute disponibilité 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
  - 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 les options avancées, à la page 300

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 multiples chemins à coûts égaux (ECMP)
- interfaces passives
- 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

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.

Configurer une interface VLAN

Cette section décrit comment configurer les interfaces VLAN à utiliser avec les ports de commutation associés. Vous devez d'abord configurer une interface VLAN pour chaque VLAN que vous souhaitez affecter à un port de commutation.



Remarque Si vous souhaitez uniquement activer la commutation entre les ports de commutation d'un VLAN donné et ne pas effectuer de routage entre ce VLAN et d'autres VLAN ou interfaces de pare-feu, laissez le champ Nom d'interface VLAN vide. Dans ce cas, vous n'avez pas non plus besoin de configurer d'adresse IP ; toute configuration IP est ignorée.

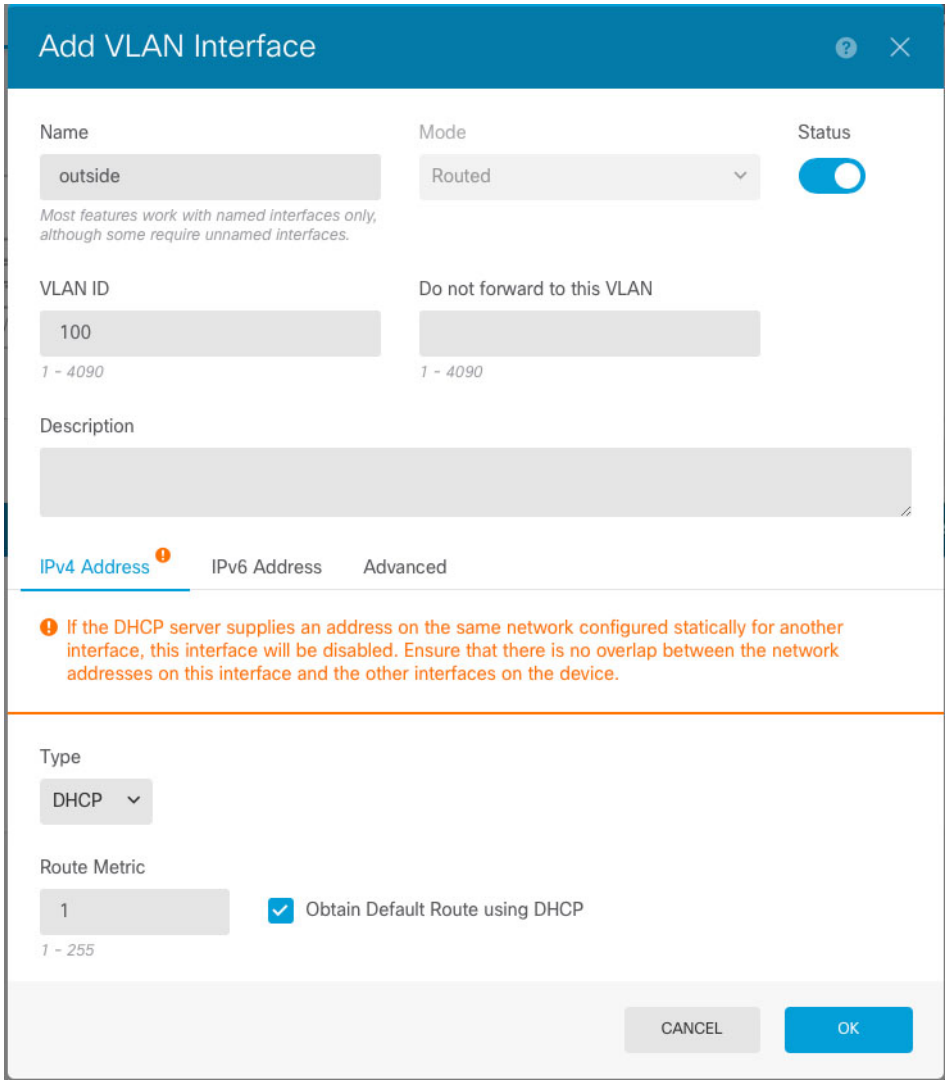
Procédure

Étape 1 Cliquez sur **Device** (Périphérique), cliquez sur le lien dans le résumé des **Interfaces**, puis cliquez sur **VLANs** (VLAN).

La liste des VLAN affiche les interfaces VLAN existantes. Cliquez sur la flèche d'ouverture/fermeture pour afficher les ports de commutation associés à chaque VLAN. Les ports de commutation sont également affichés séparément dans la page **Interfaces**.

Étape 2 Cliquez sur **Create VLAN Interface** (Créer une interface VLAN) (s'il n'y a aucun VLAN actuel) ou sur l'icône plus (+) pour créer une nouvelle interface VLAN.

Étape 3 Configurez les éléments suivants :



a) Définissez le nom de l'interface (**Interface Name**).

Définissez le nom du VLAN en utilisant au maximum 48 caractères. Les caractères alphabétiques doivent être en minuscules. Par exemple, **inside** (interne) or **outside** (externe).

Si vous ne souhaitez pas effectuer le routage entre le VLAN et d'autres VLAN ou interfaces de pare-feu, laissez le champ Nom d'interface VLAN vide.

Remarque
Si vous modifiez le nom, la modification se répercute automatiquement partout où vous avez utilisé l'ancien nom, y compris les zones de sécurité, les objets du serveur syslog et les définitions du serveur DHCP. Cependant, vous ne pouvez pas supprimer le nom avant de supprimer toutes les configurations qui utilisent le nom, car vous ne pouvez généralement pas utiliser une interface sans nom pour une politique ou un paramètre.

b) Laissez le **Mode** défini sur **Routed** (Routé).

Si vous ajoutez ultérieurement cette interface à un groupe de ponts, le mode passera automatiquement à **BridgeGroupMember** (membre du groupe de ponts). Notez que vous ne pouvez pas configurer d'adresses IP sur les interfaces des membres de groupes de ponts.

c) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

d) Définissez l'**ID VLAN** entre 1 et 4070.

Vous ne pouvez pas modifier le numéro VLAN après avoir enregistré l'interface; le numéro VLAN est à la fois la balise VLAN utilisée et l'ID d'interface dans votre configuration.

e) (Facultatif) Dans le champ **Do not forward to this VLAN** (Ne pas transférer vers ce VLAN), saisissez un ID de VLAN vers lequel cette interface VLAN ne peut pas initier de 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 depuis cette interface vers) sur le VLAN domestique ; le réseau professionnel peut accéder au réseau domestique, mais le réseau domestique ne peut pas accéder au réseau d'entreprise.

f) (Facultatif) Définissez la **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Étape 4 Cliquez sur l'onglet **IPv4 Address** (adresse IPv4) et configurez l'adresse IPv4.

Sélectionnez l'une des options suivantes dans le champ **Type** :

- **DHCP** : Sélectionnez cette option si l'adresse doit être obtenue du serveur DHCP sur le réseau. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Modifiez les options suivantes si nécessaire :
  - **Route Metric** (mesure de routage) : Si vous obtenez la voie de routage par défaut du serveur DHCP, il s'agit de la distance administrative par rapport à la route apprise (entre 1 et 255). La valeur par défaut est 1.
  - **Obtain Default Route** (obtenir la voie de routage par défaut) : Cette option permet d'obtenir la voie de routage par défaut à partir du serveur DHCP. Vous devez normalement sélectionner cette option, qui est la valeur par défaut.
- **Static** (statique) : Sélectionnez cette option si vous souhaitez affecter une adresse qui ne doit pas être modifiée. Saisissez l'adresse IP de l'interface et le masque de sous-réseau pour le réseau connecté à

l'interface. Par exemple, si vous connectez le réseau 10.100.10.0/24, vous pouvez entrer 10.100.10.1/24. Assurez-vous que l'adresse n'est pas déjà utilisée sur le réseau.

Si vous avez configuré la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IP de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

Remarque
Si un serveur DHCP est configuré pour l'interface, la configuration s'affiche. Vous pouvez modifier ou supprimer l'ensemble d'adresses DHCP. Si vous modifiez l'adresse IP de l'interface pour un sous-réseau différent, vous devez soit supprimer le serveur DHCP, soit configurer un ensemble d'adresses sur le nouveau sous-réseau, avant de pouvoir enregistrer les modifications de l'interface. Consultez Configuration du serveur DHCP, à la page 795.

- **PPPoE** : Sélectionnez cette option si l'adresse doit être obtenue à l'aide du protocole PPPoE (Point-to-point Protocol over Ethernet). PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Définissez les paramètres suivants :
  - **Group Name** (nom du groupe) : Spécifiez le nom du groupe de votre choix pour représenter cette connexion.
  - **PPPoE Username** (nom d'utilisateur PPPoE) : Spécifiez le nom d'utilisateur fourni par votre fournisseur de services Internet.
  - **PPPoE Password** : Spécifiez le mot de passe fourni par votre fournisseur de services Internet.
  - **PPP Authentication** (authentification PPP) : Choisissez **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.
  - **PPPoE Learned Route Metric** (mesure de la voie de routage apprise PPPoE) : Attribue une distance administrative à la voie de routage apprise. Cette valeur peut être comprise entre 1 et 255. Par défaut, la distance administrative pour les routes apprises est de 1.
  - **Obtain Default Route from PPPoE** (obtenir la voie de routage par défaut à partir de PPPoE) : Cochez cette case pour activer l'obtention de la voie de routage par défaut à partir du serveur PPPoE.
  - **IP Address Type (type d'adresse IP)** : Choisissez **Dynamic (dynamique)** pour obtenir l'adresse IP du serveur PPPoE. Vous pouvez également choisir **Static** (statique) si vous avez reçu une adresse IP statique du fournisseur de services Internet.

Étape 5 (Facultatif) Cliquez sur l'onglet **IPv6 Address** (adresse IPv6) et configurez l'adresse IPv6.

- **State** (état) : Pour activer le traitement IPv6 et configurer automatiquement l'adresse de liaison locale lorsque vous ne configurez pas l'adresse globale, sélectionnez **Enabled** (activé). L'adresse locale de liaison est générée en fonction des adresses MAC d'interface (format EUI-64 *modifié*).

  Remarque
  La désactivation de l'adresse IPv6 ne désactive pas le traitement IPv6 sur une interface configurée avec une adresse IPv6 explicite ou activée pour la configuration automatique.

- **Address Auto Configuration** (configuration automatique de l'adresse) : Sélectionnez cette option pour configurer l'adresse automatiquement. La configuration automatique sans état IPv6 générera une adresse IPv6 globale uniquement si le lien sur lequel le périphérique réside a un routeur configuré pour fournir des services IPv6, y compris la publicité d'un préfixe global IPv6 à utiliser sur le lien. Si les services de routage IPv6 ne sont pas disponibles sur le lien, vous obtiendrez uniquement une adresse IPv6 lien-local, à laquelle vous ne pourrez pas accéder en dehors du lien réseau immédiat de l'appareil. L'adresse locale de liaison est basée sur l'ID d'interface EUI-64 modifié.

  Bien que la RFC 4862 spécifie que les hôtes configurés pour une autoconfiguration sans état n'envoient pas de messages de publicité de routeur, le dispositif FTD envoie des messages de publicité de routeur dans ce cas. Sélectionnez **Suppress RA** (supprimer RA) pour supprimer les messages et se conformer au RFC.

- **Static Address/Prefix** (adresse statique/préfixe) : Si vous n'utilisez pas la configuration automatique sans état, saisissez l'adresse IPv6 globale statique complète et le préfixe de réseau. Par exemple : 2001:0DB8::BA98:0:3210/48. Pour en savoir plus sur l'adressage IPv6, consultez Adresse IPv6, à la page 254.

  Si vous souhaitez utiliser l'adresse comme lien local uniquement, sélectionnez l'option **Link - Local** (lien local). Les adresses locales de liaison ne sont pas accessibles en dehors du réseau local. Vous ne pouvez pas configurer une adresse lien-local sur une interface de groupe de ponts.

  Remarque
  Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. 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.

- **Standby IP Address** (adresse IP en veille) : Si vous configurez la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IPv6 de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

- **Suppress RA** : Cette option permet de supprimer les publicités de routeur. FTD peut participer à des publicités de routeur afin que les dispositifs voisins puissent apprendre de façon dynamique une adresse de routeur par défaut. Par défaut, des messages de publicité de routeur (ICMPv6 type 134) sont envoyés périodiquement à chaque interface configurée IPv6.

  Des publicités de routeur sont également envoyées en réponse à des 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 supprimer ces messages sur toute interface dont vous ne souhaitez pas que le dispositif FTD fournisse le préfixe IPv6 (par exemple, l'interface externe).

Étape 6 (Facultatif) Configurer les options avancées, à la page 300.

Les paramètres avancés comprennent des paramètres par défaut appropriés pour la plupart des réseaux. Modifiez-les uniquement lors de la résolution des problèmes de réseau.

Étape 7 Cliquez sur **OK**.

Prochaine étape

- Ajoutez les VLAN aux zones de sécurité appropriées. Consultez Configuration des zones de sécurité, à la page 148.

Configurer les ports de commutation comme ports d'accès

Pour affecter un port de commutation à un seul VLAN, configurez-le comme port d'accès. Par défaut, Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation activés et affectés au VLAN 1 sur le Firepower 1010 et le Secure Firewall 1210

Remarque Le Firepower 1010 ne prennent 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 le périphérique Firewall Threat Defense ne finit pas dans une boucle de réseau.

Avant de commencer

Ajoutez une interface VLAN pour l'ID du VLAN auquel vous souhaitez affecter le port d'accès. Les ports d'accès acceptent uniquement le trafic non balisé. Consultez Configurer une interface VLAN, à la page 278.

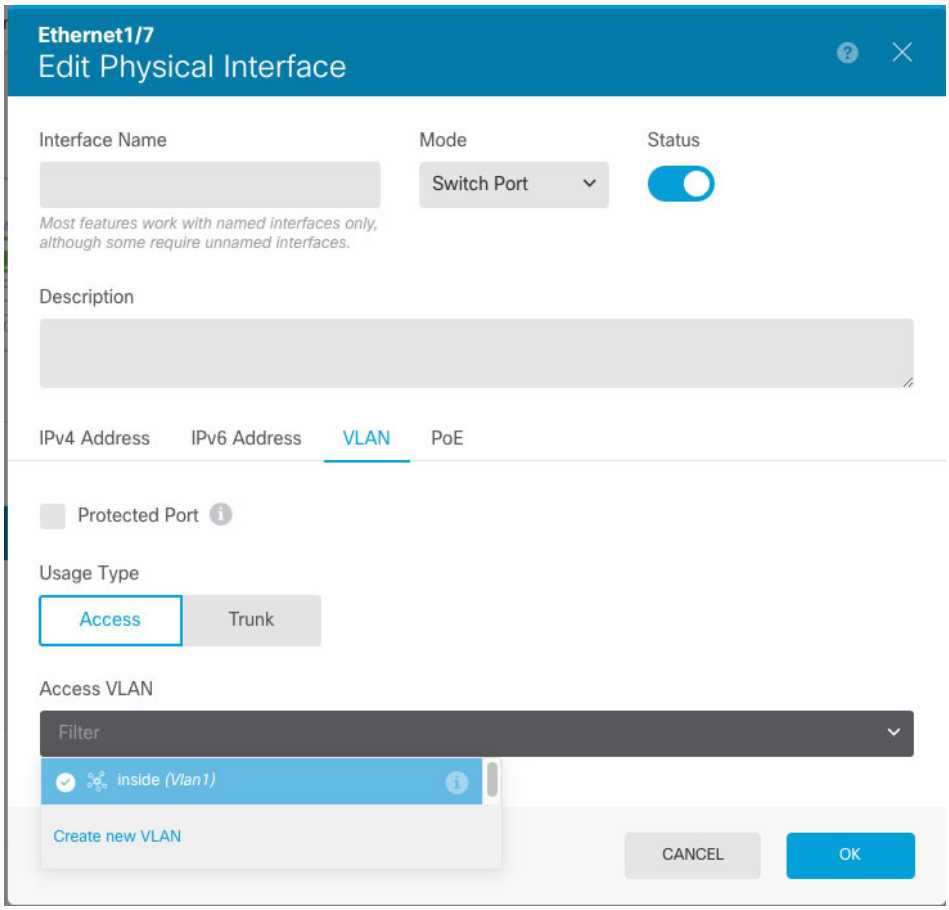
Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé des **Interfaces**.

La page **Interfaces** est sélectionnée par défaut. La liste des interfaces affiche les interfaces physiques : leurs noms, adresses et états.

Étape 2 Cliquez sur l'icône de modification ( ) pour l'interface physique que vous souhaitez modifier.

Étape 3 Définissez les paramètres suivants :



a) Ne définissez pas **Interface Name** (Nom d'interface) pour les ports de commutation ; seule l'interface VLAN associée est une interface nommée.

b) Définissez le champ **Mode** sur **Switch Por**t (Port de commutation).

c) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

d) (Facultatif) Définissez la **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Étape 4 Cliquez sur **VLAN** pour définir les éléments suivants :

a) (Facultatif) Cochez la case **Protected Port** (Port protégé) pour définir ce port de commutation comme protégé, afin de 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 si vous appliquez cette option à chaque port de commutateur. 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.

b) Pour **Usage Type** (Type d'utilisation, cliquez sur **Access** (Accès).

c) Pour **Access VLAN** (VLAN d'accès), cliquez sur la flèche vers le bas pour choisir l'une des interfaces VLAN existantes.

Vous pouvez ajouter une nouvelle interface VLAN en cliquant sur **Create new VLAN** (Créer un nouveau VLAN). Consultez Configurer une interface VLAN, à la page 278

Étape 5 Cliquez sur **OK**.

Configurer les 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 le port de ligne principale reçoit un trafic non balisé, il le balise à l'ID de VLAN natif afin que le périphérique puisse transférer le trafic vers les ports de commutation appropriés ou l'acheminer vers une autre interface de pare-feu. Lorsque le périphérique envoie le trafic d'ID de VLAN natif hors du port de ligne principale, 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.

Avant de commencer

Ajoutez une interface VLAN pour chaque ID de VLAN auquel vous souhaitez affecter le port de ligne principale. Consultez Configurer une interface VLAN, à la page 278.

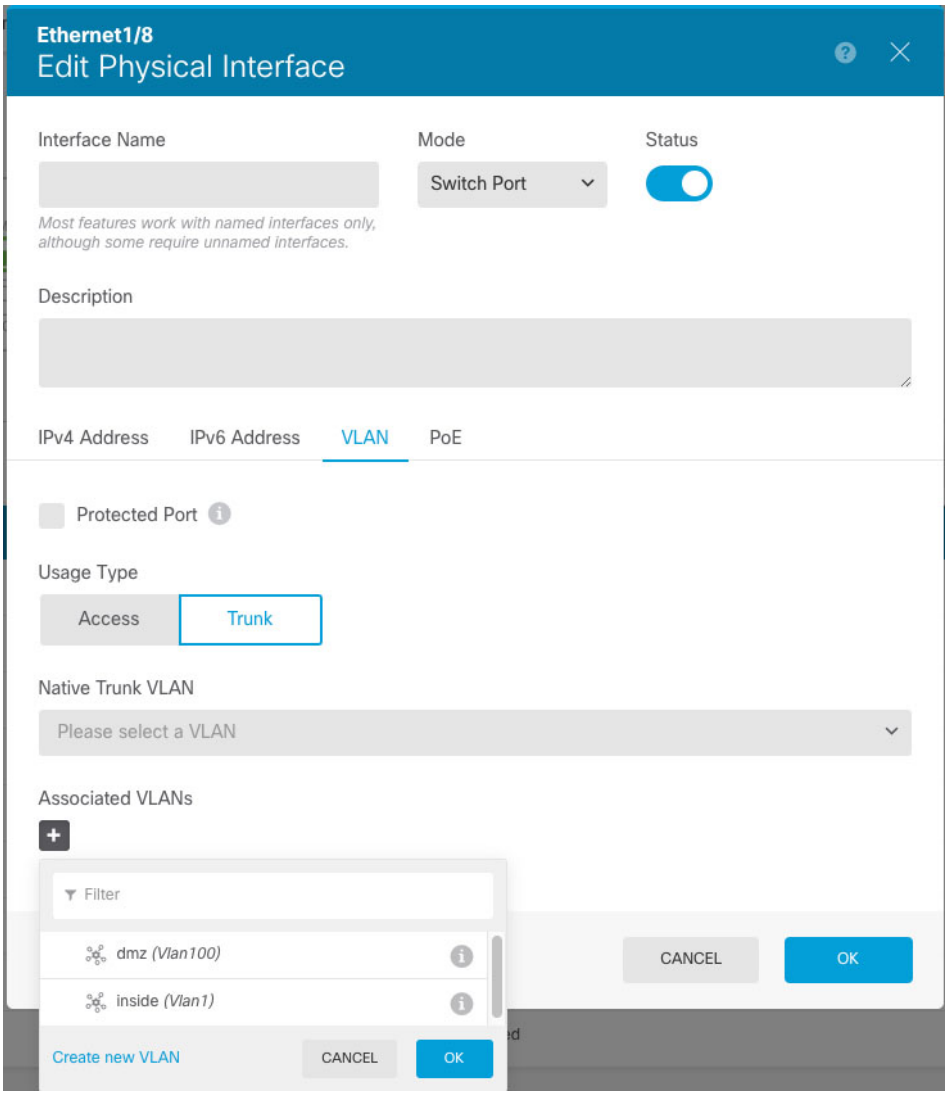
Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé des **Interfaces**.

La page **Interfaces** est sélectionnée par défaut. La liste des interfaces affiche les interfaces physiques : leurs noms, adresses et états.

Étape 2 Cliquez sur l'icône de modification () pour l'interface physique que vous souhaitez modifier.

Étape 3 Définissez les paramètres suivants :



a) Ne définissez pas **Interface Name** (Nom d'interface) pour les ports de commutation ; seule l'interface VLAN associée est une interface nommée.

b) Définissez le champ **Mode** sur **Switch Por**t (Port de commutation).

c) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

d) (Facultatif) Définissez la **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Étape 4 Cliquez sur **VLAN** pour définir les éléments suivants :

a) (Facultatif) Cochez la case **Protected Port** (Port protégé) pour définir ce port de commutation comme protégé, afin de 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 si vous appliquez cette option à chaque port de commutateur. 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.

b) Pour **Usage Type** (Type d'utilisation, cliquez sur **Trunk**.

c) (Facultatif) Pour **Native Trunk VLAN** (VLAN de tronc natif), cliquez sur la flèche vers le bas pour choisir l'une des interfaces VLAN existantes pour le VLAN natif.

L'ID VLAN natif par défaut est 1.

Chaque port ne peut avoir qu'un seul VLAN natif, mais chaque port peut avoir le même VLAN natif ou un différent.

Vous pouvez ajouter une nouvelle interface VLAN en cliquant sur **Create new VLAN** (Créer un nouveau VLAN). Consultez Configurer une interface VLAN, à la page 278.

d) Pour **Associated VLANs** (VLAN associés), cliquez sur l'icône plus ( ) pour sélectionner une ou plusieurs interfaces VLAN existantes.

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.

Vous pouvez ajouter une nouvelle interface VLAN en cliquant sur **Create new VLAN** (Créer un nouveau VLAN). Consultez Configurer une interface VLAN, à la page 278

Étape 5 Cliquez sur **OK**.

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.

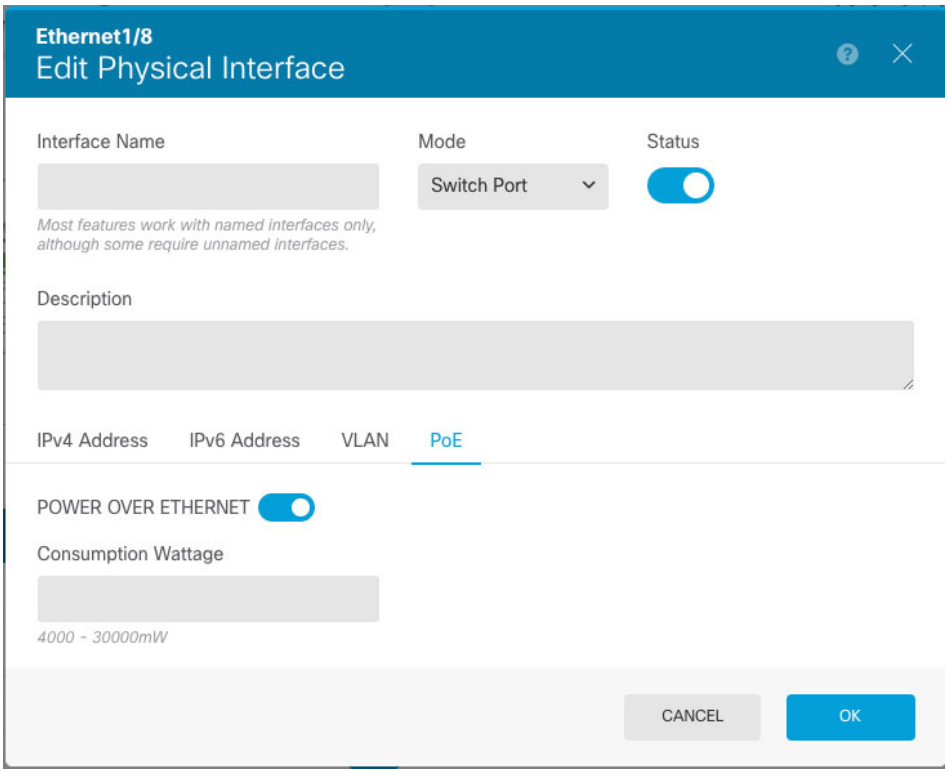
Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé des **Interfaces**.

La page **Interfaces** est sélectionnée par défaut. La liste des interfaces affiche les interfaces physiques : leurs noms, adresses et états.

Étape 2 Cliquez sur l'icône de modification ( ) pour Ethernet1/7 ou 1/8.

Étape 3 Cliquez sur **PoE**, et définissez les éléments suivants :



a) Pour activer **Power over Ethernet** (alimentation électrique par Ethernet), cliquez sur le curseur ( ) afin de l'activer.

Le mode PoE est activé par défaut.

b) (Facultatif) Saisissez la **consommation en watts** si vous connaissez la puissance exacte dont vous avez besoin.

Pour configurer manuellement, spécifiez la puissance en milliwatts, de 4 000 à 30 000. Utilisez cette option si vous souhaitez définir les watts manuellement et désactiver la négociation LLDP. Pour l'attribution manuelle, la classe s'affichera dans la sortie **show power inline** comme **n/a** car la classe n'est pas utilisée pour déterminer la consommation d'énergie.

Par défaut, PoE 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. Lorsque vous connectez un périphérique d'une certaine classe, il sera provisionné au maximum pour cette classe au cas où il aurait besoin d'utiliser plus de puissance. Par exemple, si vous ajoutez un périphérique de classe 4 qui demande 12,95 W, il se verra attribuer 30 W même s'il n'utilise pas actuellement toute cette puissance. Certains appareils peuvent renégocier les besoins en matière d'alimentation. Si vous savez que votre périphérique a besoin de moins d'alimentation que ce qui est alloué, vous pouvez plutôt définir la **consommation en watts** manuellement pour libérer de l'alimentation pour d'autres périphériques.

Étape 4 Cliquez sur **OK**.

Configurer les sous-interfaces VLAN et la jonction 802.1Q

Les sous-interfaces VLAN vous permettent de diviser une interface physique 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 de périphériques supplémentaires.

Créez des sous-interfaces si vous connectez l'interface physique à un port de ligne principale sur un commutateur. Créez une sous-interface pour chaque réseau VLAN pouvant apparaître sur le port de ligne principale du commutateur. Si vous connectez l'interface physique à un port d'accès sur le commutateur, il est inutile de créer une sous-interface.

Lignes directrices et limites relatives à la licence

- 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. Étant donné que l'interface physique doit être activée pour que la sous-interface achemine le trafic, assurez-vous que l'interface physique ne transmet pas le trafic en ne nommant pas l'interface. Si vous souhaitez laisser l'interface physique passer des paquets non étiquetés, vous pouvez nommer l'interface comme d'habitude.
- 1010 : les sous-interfaces ne sont pas prises en charge sur les ports de commutation ou les interfaces VLAN.
- Vous ne pouvez pas configurer d'adresses IP sur les interfaces de membre de groupe de passerelle, mais vous pouvez modifier les paramètres avancés au besoin.
- 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.
- Firewall Threat Defense ne prend pas en charge le protocole DTP (Dynamic Trunking Protocol), vous devez donc configurer le port du commutateur connecté pour qu'il puisse établir une liaison sans condition.
- Vous pouvez vouloir attribuer des adresses MAC uniques aux sous-interfaces définies sur le périphérique Firepower Threat Defense, car elles utilisent la même adresse MAC gravée de l'interface parent. 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 Firepower Threat Defense.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé des **Interfaces**.

La page **Interfaces** est sélectionnée par défaut. Pour ajouter une sous-interface à un canal EtherChannel, cliquez sur **EtherChannel**. La liste des interfaces affiche les interfaces physiques : leurs noms, adresses et états.

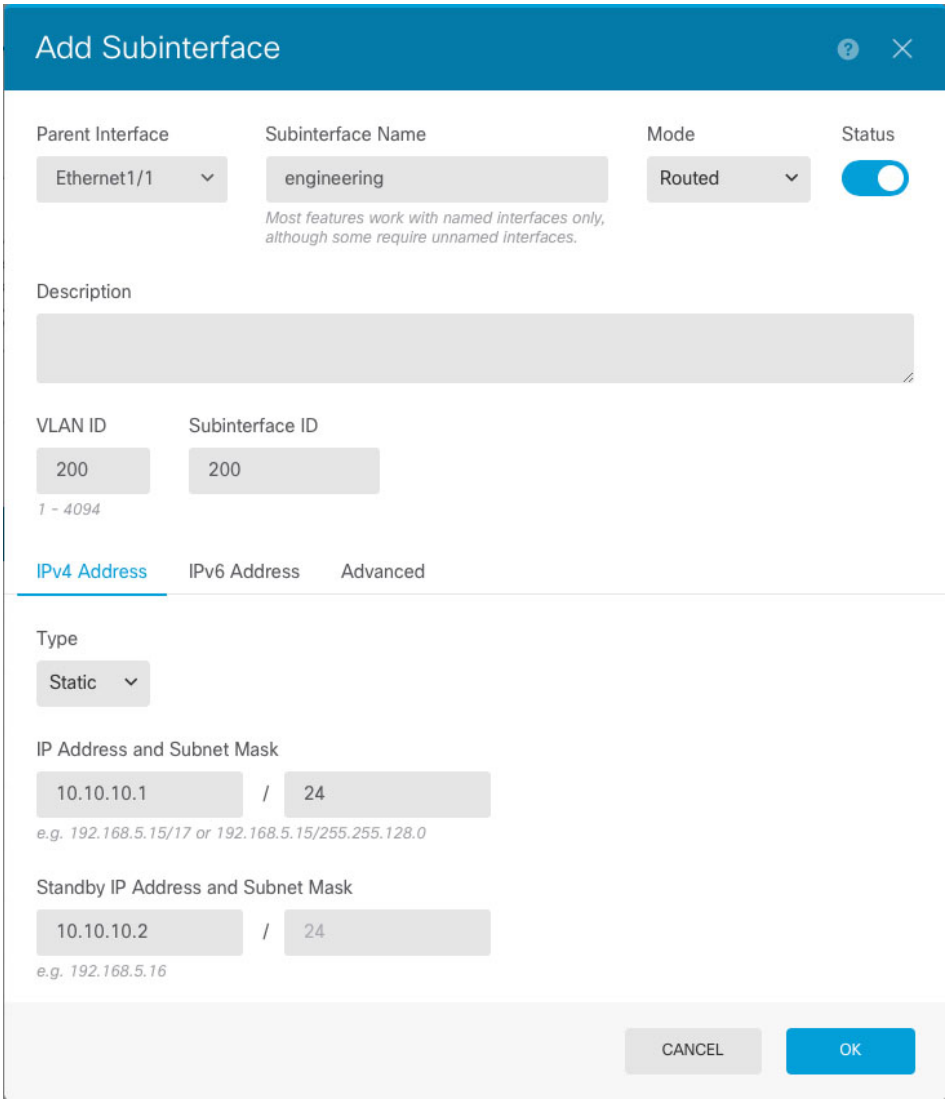
Étape 2 Effectuez l'une des opérations suivantes :

- Dans la page des **Interfaces**, cliquez sur l'icône plus (+) pour créer une nouvelle sous-interface.
- Sur la page **EtherChannel**, cliquez sur l'icône de flèche vers le haut et vers le bas (+), puis sélectionnez **Subinterface** (sous-interface).
- Cliquez sur l'icône de modification () pour la sous-interface que vous souhaitez modifier.

Si vous n'avez plus besoin d'une sous-interface, cliquez sur l'icône de suppression () pour la supprimer.

Étape 3 Définissez le curseur **Status** (état) selon sur le paramètre activé ().

Étape 4 Configurez l'interface parente en précisant son nom et en indiquant une description :



a) Choisissez l'interface parente **Parent Interface**.

L'interface parente est l'interface physique à laquelle vous souhaitez ajouter la sous-interface. Vous ne pouvez pas modifier l'interface parente après avoir créé la sous-interface.

b) Définissez le nom de la sous-interface (**Subinterface Name**) en utilisant au maximum 48 caractères.

Les caractères alphabétiques doivent être en minuscules. Par exemple, **inside** (interne) or **outside** (externe). Sans nom, le reste de la configuration de l'interface est ignoré.

Remarque
Si vous modifiez le nom, la modification se répercute automatiquement partout où vous avez utilisé l'ancien nom, y compris les zones de sécurité, les objets du serveur syslog et les définitions du serveur DHCP. Cependant, vous ne pouvez pas supprimer le nom avant de supprimer toutes les configurations qui utilisent le nom, car vous ne pouvez généralement pas utiliser une interface sans nom pour une politique ou un paramètre.

c) Réglez le **Mode** sur **Routed** (routé).

Si vous ajoutez ultérieurement cette interface à un groupe de ponts, le mode passera automatiquement à **BridgeGroupMember** (membre du groupe de ponts). Notez que vous ne pouvez pas configurer d'adresses IP sur les interfaces des membres de groupes de ponts.

d) (Facultatif) Définissez la **description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

e) Définissez le numéro VLAN (**VLAN ID**).

Entrez le numéro du VLAN entre 1 et 4094 qui sera utilisé pour baliser les paquets sur cette sous-interface.

f) Définissez l'ID de sous-interface (**Subinterface ID**).

Entrez l'ID de la sous-interface comme un nombre entier entre 1 et 4294967295. Cet ID est ajouté à l'ID de l'interface; par exemple Ethernet 1/1.100. Vous pouvez faire correspondre le numéro VLAN pour plus de commodité, mais ce n'est pas obligatoire. Vous ne pouvez pas modifier l'ID après avoir créé la sous-interface.

Étape 5 Cliquez sur l'onglet **IPv4 Address** (adresse IPv4) et configurez l'adresse IPv4.

Sélectionnez l'une des options suivantes dans le champ **Type** :

- **DHCP** : Sélectionnez cette option si l'adresse doit être obtenue du serveur DHCP sur le réseau. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Modifiez les options suivantes si nécessaire :
  - **Route Metric** (mesure de routage) : Si vous obtenez la voie de routage par défaut du serveur DHCP, il s'agit de la distance administrative par rapport à la route apprise (entre 1 et 255). La valeur par défaut est 1.
  - **Obtain Default Route** (obtenir la voie de routage par défaut) : Cette option permet d'obtenir la voie de routage par défaut à partir du serveur DHCP. Vous devez normalement sélectionner cette option, qui est la valeur par défaut.
- **Static** (statique) : Sélectionnez cette option si vous souhaitez affecter une adresse qui ne doit pas être modifiée. Saisissez l'adresse IP de l'interface et le masque de sous-réseau pour le réseau connecté à l'interface. Par exemple, si vous connectez le réseau 10.100.10.0/24, vous pouvez entrer 10.100.10.1/24. Assurez-vous que l'adresse n'est pas déjà utilisée sur le réseau.

  Si vous avez configuré la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IP de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

Remarque
Si un serveur DHCP est configuré pour l'interface, la configuration s'affiche. Vous pouvez modifier ou supprimer l'ensemble d'adresses DHCP. Si vous modifiez l'adresse IP de l'interface pour un sous-réseau différent, vous devez soit supprimer le serveur DHCP, soit configurer un ensemble d'adresses sur le nouveau sous-réseau, avant de pouvoir enregistrer les modifications de l'interface. Consultez Configuration du serveur DHCP, à la page 795.

- **PPPoE** : Sélectionnez cette option si l'adresse doit être obtenue à l'aide du protocole PPPoE (Point-to-point Protocol over Ethernet). PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Définissez les paramètres suivants :
  - **Group Name** (nom du groupe) : Spécifiez le nom du groupe de votre choix pour représenter cette connexion.
  - **PPPoE Username** (nom d'utilisateur PPPoE) : Spécifiez le nom d'utilisateur fourni par votre fournisseur de services Internet.
  - **PPPoE Password** : Spécifiez le mot de passe fourni par votre fournisseur de services Internet.
  - **PPP Authentication** (authentification PPP) : Choisissez **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.
  - **PPPoE Learned Route Metric** (mesure de la voie de routage apprise PPPoE) : Attribue une distance administrative à la voie de routage apprise. Cette valeur peut être comprise entre 1 et 255. Par défaut, la distance administrative pour les routes apprises est de 1.
  - **Obtain Default Route from PPPoE** (obtenir la voie de routage par défaut à partir de PPPoE) : Cochez cette case pour activer l'obtention de la voie de routage par défaut à partir du serveur PPPoE.
  - **IP Address Type (type d'adresse IP)** : Choisissez **Dynamic (dynamique)** pour obtenir l'adresse IP du serveur PPPoE. Vous pouvez également choisir **Static** (statique) si vous avez reçu une adresse IP statique du fournisseur de services Internet.

Étape 6 (Facultatif) Cliquez sur l'onglet **IPv6 Address** (adresse IPv6) et configurez l'adresse IPv6.

- **State** (état) : Pour activer le traitement IPv6 et configurer automatiquement l'adresse de liaison locale lorsque vous ne configurez pas l'adresse globale, sélectionnez **Enabled** (activé). L'adresse locale de liaison est générée en fonction des adresses MAC d'interface (format EUI-64 *modifié*).

Remarque
La désactivation de l'adresse IPv6 ne désactive pas le traitement IPv6 sur une interface configurée avec une adresse IPv6 explicite ou activée pour la configuration automatique.

- **Address Auto Configuration** (configuration automatique de l'adresse) : Sélectionnez cette option pour configurer l'adresse automatiquement. La configuration automatique sans état IPv6 générera une adresse IPv6 globale uniquement si le lien sur lequel le périphérique réside a un routeur configuré pour fournir des services IPv6, y compris la publicité d'un préfixe global IPv6 à utiliser sur le lien. Si les services de routage IPv6 ne sont pas disponibles sur le lien, vous obtiendrez uniquement une adresse IPv6 lien-local, à laquelle vous ne pourrez pas accéder en dehors du lien réseau immédiat de l'appareil. L'adresse locale de liaison est basée sur l'ID d'interface EUI-64 modifié.

  Bien que la RFC 4862 spécifie que les hôtes configurés pour une autoconfiguration sans état n'envoient pas de messages de publicité de routeur, le dispositif FTD envoie des messages de publicité de routeur dans ce cas. Sélectionnez **Suppress RA** (supprimer RA) pour supprimer les messages et se conformer au RFC.

- **Static Address/Prefix** (adresse statique/préfixe) : Si vous n'utilisez pas la configuration automatique sans état, saisissez l'adresse IPv6 globale statique complète et le préfixe de réseau. Par exemple : 2001:0DB8::BA98:0:3210/48. Pour en savoir plus sur l'adressage IPv6, consultez Adresse IPv6, à la page 254.

  Si vous souhaitez utiliser l'adresse comme lien local uniquement, sélectionnez l'option **Link - Local** (lien local). Les adresses locales de liaison ne sont pas accessibles en dehors du réseau local. Vous ne pouvez pas configurer une adresse lien-local sur une interface de groupe de ponts.

  Remarque
  Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. 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.

- **Standby IP Address** (adresse IP en veille) : Si vous configurez la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IPv6 de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

- **Suppress RA** : Cette option permet de supprimer les publicités de routeur. FTD peut participer à des publicités de routeur afin que les dispositifs voisins puissent apprendre de façon dynamique une adresse de routeur par défaut. Par défaut, des messages de publicité de routeur (ICMPv6 type 134) sont envoyés périodiquement à chaque interface configurée IPv6.

  Des publicités de routeur sont également envoyées en réponse à des 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 supprimer ces messages sur toute interface dont vous ne souhaitez pas que le dispositif FTD fournisse le préfixe IPv6 (par exemple, l'interface externe).

Étape 7 (Facultatif) Configurer les options avancées, à la page 300.

Les paramètres avancés comprennent des paramètres par défaut appropriés pour la plupart des réseaux. Modifiez-les uniquement lors de la résolution des problèmes de réseau.

Étape 8 Cliquez sur **OK**.

Prochaine étape

- Ajoutez les sous-interfaces aux zones de sécurité appropriées. Consultez Configuration des zones de sécurité, à la page 148.

Configurer des interfaces passives

Les interfaces passives surveillent le trafic circulant sur un réseau à l'aide d'un commutateur SPAN ou d'un port miroir. Le port SPAN ou miroir permet de copier le trafic d'autres ports du commutateur. Cette fonction assure la visibilité du système dans le réseau sans être dans le flux du trafic réseau.

Lorsqu'il est configuré dans un déploiement passif, le système ne peut pas prendre certaines mesures telles que le blocage du trafic. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis.

Vous utilisez une interface passive pour surveiller le trafic sur le réseau afin de recueillir des informations sur le trafic. Par exemple, vous pouvez appliquer des politiques de prévention des intrusions pour identifier les types de menaces qui affectent le réseau ou pour voir les catégories d'URL pour les demandes Web des utilisateurs. Vous pouvez mettre en œuvre diverses politiques et règles de sécurité pour voir ce que ferait le système s'il était déployé activement, afin qu'il puisse abandonner le trafic en fonction de votre contrôle d'accès et d'autres règles.

Cependant, comme les interfaces passives ne peuvent pas avoir d'incidence sur le trafic, il existe de nombreuses limites de configuration. Ces interfaces laissent simplement le système surveiller le trafic : aucun paquet qui entre dans une interface passive ne quitte le périphérique.

Les rubriques suivantes expliquent plus en détail les interfaces passives et comment les configurer.

Interfaces passives

L'objectif principal des interfaces passives est de fournir un mode de démonstration simple. Vous pouvez configurer le commutateur pour surveiller un seul port source, puis utiliser un poste de travail pour envoyer le trafic de test surveillé par l'interface passive. Ainsi, vous pouvez voir comment le système Firepower Threat Defense évalue les connexions, identifie les menaces, etc. Une fois que vous êtes satisfait des performances du système, vous pouvez le déployer activement dans votre réseau et supprimer la configuration d'interface passive.

Cependant, vous pouvez également utiliser des interfaces passives dans un environnement de production pour fournir les services suivants :

- Déploiement d'IDS pur : si vous ne souhaitez pas utiliser le système comme pare-feu ou IPS (système de prévention des intrusions), vous pouvez le déployer de manière passive en tant qu'IDS (système de détection d'intrusion) . Dans cette méthode de déploiement, vous utiliseriez une règle de contrôle d'accès pour appliquer une politique de prévention des intrusions à tout le trafic. Le système surveillerait également plusieurs ports sources sur le commutateur. Ensuite, vous pourrez utiliser les tableaux de bord pour surveiller les menaces vues sur le réseau. Cependant, dans ce mode, le système ne peut rien faire pour empêcher ces menaces.

- Déploiement mixte : vous pouvez combiner des interfaces routées actives avec des interfaces passives sur le même système. Ainsi, vous pouvez déployer le périphérique Firepower Threat Defense en tant que pare-feu dans certains réseaux, tout en configurant une ou plusieurs interfaces passives pour surveiller le trafic dans d'autres réseaux.

Limites pour les interfaces passives

Toute interface physique que vous définissez comme interface en mode passif a les restrictions suivantes :

- Vous ne pouvez pas configurer de sous-interfaces sur l'interface passive.
- Vous ne pouvez pas ajouter une interface en mode passif à un groupe de pont.
- Vous ne pouvez pas configurer les adresses IPv4 ou IPv6 sur une interface passive.
- Vous ne pouvez pas sélectionner l'option Management Only (Gestion uniquement) pour une interface passive.
- Vous pouvez inclure l'interface dans une zone de sécurité en mode passif uniquement, vous ne pouvez pas l'inclure dans une zone de sécurité routée.
- Vous pouvez inclure des zones de sécurité passive dans les critères de source des règles de contrôle d'accès ou d'identité. Vous ne pouvez pas utiliser de zones passives dans les critères de destination. Vous ne pouvez pas combiner des zones de sécurité passives et routées dans une seule règle.
- Vous ne pouvez pas configurer de règles d'accès de gestion (HTTPS ou SSH) pour une interface passive.
- Vous ne pouvez pas utiliser une interface en mode passif dans les règles NAT.
- Vous ne pouvez pas configurer de routes statiques pour une interface passive. Vous ne pouvez pas non plus utiliser une interface passive dans la configuration d'un protocole de routage.
- Vous ne pouvez pas configurer un serveur DHCP sur une interface en mode passif. Vous ne pouvez pas non plus utiliser une interface passive pour obtenir des paramètres DHCP par le biais de la configuration automatique.
- Vous ne pouvez pas utiliser une interface passive dans une configuration de serveur syslog.
- Vous ne pouvez pas configurer de type de VPN sur une interface passive.

Configurer le commutateur pour une interface matérielle FTD passive

Une interface passive sur du matériel Firepower Threat Defense ne fonctionne que si vous configurez correctement le commutateur de réseau. La procédure suivante est basée sur un commutateur de la gamme Cisco Nexus 5000. Si vous avez un autre type de commutateur, les commandes pourraient différer.

L'idée de base consiste à configurer un port SPAN (Switched Port Analyzer) ou miroir, à connecter l'interface passive à ce port et à configurer une session de surveillance sur le commutateur pour envoyer des copies du trafic d'un ou de plusieurs ports sources au port SPAN ou miroir.

Procédure

Étape 1 Configurez un port du commutateur comme port de surveillance (SPAN ou miroir).

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)#
```

Étape 2 Définissez une session de surveillance pour définir les ports à surveiller.

Assurez-vous de définir le port SPAN ou miroir comme port de destination. Dans l'exemple suivant, deux ports source sont surveillés.

```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

Étape 3 (Facultatif) Vérifiez la configuration à l'aide de la commande **show monitor session**.

L'exemple suivant présente la sortie brève pour la session 1.

```
switch# show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

Étape 4 Connectez physiquement le câble de l'interface passive Firepower Threat Defense au port de destination du commutateur.

Vous pouvez configurer l'interface en mode passif avant ou après la connexion physique. Consultez Configurer l'interface physique en mode passif, à la page 297.

Configurer le VLAN pour une interface passive FTDv

Une interface passive sur un périphérique FTDv ne fonctionne que si vous configurez correctement le réseau VLAN sur le réseau virtuel. Assurez-vous de procéder comme suit :

- Connectez l'interface FTDv à un réseau VLAN que vous avez configuré en mode promiscuité. Ensuite, configurez l'interface comme expliqué dans Configurer l'interface physique en mode passif, à la page 297. L'interface passive verra une copie de tout le trafic sur le VLAN en mode promiscuité.
- Sur le même réseau VLAN, connectez un ou plusieurs périphériques d'extrémité, tels que des systèmes Windows virtuels. Vous pouvez utiliser un seul périphérique s'il y a une connexion du VLAN à Internet. Sinon, vous avez besoin d'au moins deux appareils pour transmettre le trafic entre eux. Pour obtenir des données pour les catégories d'URL, vous devez avoir une connexion Internet.

Configurer l'interface physique en mode passif

Vous pouvez configurer une interface en mode passif. Lorsqu'elle agit de manière passive, l'interface surveille simplement le trafic provenant des ports source dans le cadre d'une session de surveillance configurée sur le commutateur lui-même (pour les périphériques matériels) ou sur le réseau VLAN en mode promiscuité (pour Firewall Threat Defense Virtual). Pour obtenir des informations détaillées sur ce que vous devez configurer dans le commutateur ou le réseau virtuel, consultez les rubriques suivantes :

- Configurer le commutateur pour une interface matérielle FTD passive, à la page 295
- Configurer le VLAN pour une interface passive FTDv, à la page 296

Utilisez le mode passif lorsque vous souhaitez analyser le trafic entrant par les ports de commutation surveillés sans impact sur le trafic. Pour un exemple de bout en bout d'utilisation du mode passif, consultez Comment surveiller passivement le trafic sur un réseau, à la page 78.

Procédure

Étape 1 Cliquez sur **Device** (périphérique), puis sur le lien dans le résumé des **interfaces**. Cliquez ensuite sur **Interfaces** ou **EtherChannels**.

Étape 2 Cliquez sur l'icône de modification ( ) pour l'interface physique ou le port EtherChannel que vous souhaitez modifier.

Choisissez une interface actuellement inutilisée. Si vous avez l'intention de convertir une interface en cours d'utilisation en interface passive, vous devez d'abord supprimer l'interface de toute zone de sécurité et supprimer toutes les autres configurations qui utilisent l'interface.

Étape 3 Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

Étape 4 Configurez les éléments suivants :

- **Interface Name** : le nom de l'interface (jusqu'à 48 caractères). Les caractères alphabétiques doivent être en minuscules. Par exemple, surveiller.
- **Mode** : Sélectionnez **Passive** (passif).
- (Facultatif) **Description** : La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Remarque
Vous ne pouvez pas configurer les adresses IPv4 ou IPv6. Sous l'onglet des paramètres avancés, vous pouvez modifier uniquement les paramètres MTU, duplex et de vitesse.

Étape 5 Cliquez sur **OK**.

Prochaine étape

La création d'une interface passive n'est pas suffisante pour remplir les tableaux de bord avec les informations sur le trafic vu sur l'interface. Vous devez également procéder comme précisé ci-après. Le scénarios d'utilisation traitent de ces étapes. Consultez Comment surveiller passivement le trafic sur un réseau, à la page 78.

- Créez une zone de sécurité passive et ajoutez-y l'interface. Consultez Configuration des zones de sécurité, à la page 148.
- Créez des règles de contrôle d'accès qui utilisent la zone de sécurité passive comme zone source. En règle générale, vous devez appliquer des politiques d'intrusion dans ces règles pour mettre en œuvre la surveillance IDS (système de détection d'intrusion). Consultez Configuration de la politique de contrôle d'accès, à la page 515.
- Vous pouvez également créer des règles d'identité et de déchiffrement SSL pour la zone de sécurité passive et activer la politique de renseignement de sécurité.

Configurer les options d'interface avancées

Les options avancées comprennent la définition de l'unité de transfert maximale (MTU), des paramètres matériels, du mode gestion uniquement, de l'adresse MAC et d'autres paramètres.

À propos des adresses MAC

Vous pouvez configurer manuellement des adresses Media Access Control (MAC) afin de remplacer la valeur par défaut.

Pour une configuration de haute disponibilité, vous pouvez configurer, pour une interface, l'adresse MAC active et l'adresse MAC de secours. 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.

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) —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 la section Configurer les options avancées, à la page 300.
- EtherChannels pour un 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. 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.

- 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 FTD.

À propos de la MTU

La MTU spécifie la taille maximale de la *charge utile* de trame que l' Appareil FTD 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.

Chemin de découverte de MTU

L' Appareil FTD 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 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 UDP ou ICMP, l'application doit prendre en compte la MTU pour éviter la fragmentation.



Remarque L' Appareil FTD 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 FTD et les autres interfaces de périphériques le long du chemin de trafic. La correspondance des MTU empêche les périphériques intermédiaires de fragmenter les paquets.
- 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 définir la MTU à 9 000 octets ou plus pour la prise en charge des trames étendues. Le maximum dépend du modèle.

Remarque L'augmentation de la MTU affecte plus de mémoire aux trames étendues, ce qui peut limiter l'utilisation maximale d'autres fonctions, telles que les règles d'accès. Si vous augmentez le MTU au-delà de 1500 sur des périphériques de la série ASA 5500-X, des périphériques de la série ISA 3000, ou Firewall Threat Defense Virtual, vous devez redémarrer le périphérique. Si le périphérique est configuré pour la haute disponibilité, vous devez également redémarrer le périphérique en veille. Vous n'avez pas besoin de redémarrer les autres modèles, où la prise en charge des trames étendues est toujours activée.

Configurer les options avancées

Les options d'interface avancées ont des paramètres par défaut adaptés à la plupart des réseaux. Ne les configurez que si vous résolvez des problèmes de réseau ou si vous configurez la haute disponibilité.

La procédure suivante suppose que l'interface est déjà définie. Vous pouvez également modifier ces paramètres lors de la modification ou de la création de l'interface.

Restrictions

- Pour les groupes de ponts, vous configurez la plupart de ces options sur les interfaces membres. À l'exception des tentatives DAD et de l'option Enable for HA Monitoring (activer pour), ces options ne sont pas disponibles pour l'interface virtuelle de pont (BVI).
- Vous ne pouvez pas définir le MTU, les conditions de duplex ou la vitesse pour l'interface de gestion sur un appareil Firepower 1000 ou 2100.
- Les options avancées ne sont pas disponibles pour les ports de commutateur Firepower 1010.
- Vous ne pouvez pas définir les conditions de duplex ou la vitesse pour les interfaces sur le Firepower 4100/9300. Définissez ces fonctionnalités pour l'interface avec FXOS.
- Pour les interfaces passives, vous pouvez définir uniquement la MTU, le duplex et la vitesse. Vous ne pouvez pas effectuer uniquement la gestion de l'interface.

Procédure

Étape 1 Cliquez sur **Device** (périphérique), cliquez sur le lien dans le résumé des **Interfaces**. Cliquez ensuite sur le type d'interfaces pour consulter la liste des interfaces.

Étape 2 Cliquez sur l'icône de modification ( ) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur **Advanced Options** (options avancées).

Étape 4 Sélectionnez **Enable for HA Monitoring** (activer pour la surveillance haute disponibilité) si vous souhaitez que l'intégrité de l'interface soit prise en compte lorsque le système décide de basculer vers l'unité homologue dans une configuration à haute disponibilité.

Cette option est ignorée si vous ne configurez pas la haute accessibilité. Elle est également ignorée si vous ne configurez pas de nom pour l'interface.

Étape 5 Pour assurez la gestion de l'interface de données uniquement, sélectionnez **Management Only** (gestion uniquement).

Une interface de gestion uniquement ne permet pas le trafic traversant, il est donc très peu utile de définir une interface de données pour la gestion uniquement. Vous ne pouvez pas modifier ce paramètre pour l'interface de gestion/diagnostic, qui se destine toujours à la gestion uniquement.

Étape 6 Modifiez la **MTU** (unité de transmission maximale) à la valeur souhaitée.

Par défaut, la MTU est de 1500 octets. Le minimum et le maximum dépendent de votre plateforme. Définissez une valeur élevée si vous voyez généralement des trames étendues sur votre réseau.

Remarque
Si vous augmentez le MTU au-delà de 1500 sur les périphériques suivants, vous devez redémarrer le périphérique : Périphériques de la série ASA 5500-X, Périphériques de la série ISA 3000,FTDv. Si le périphérique est configuré pour la haute disponibilité, vous devez également redémarrer le périphérique en veille. Vous n'avez pas besoin de redémarrer les autres modèles, où la prise en charge des trames étendues est toujours activée.

Étape 7 (Interface physique uniquement.) Modifiez les paramètres de vitesse et de duplex.

Par défaut, l'interface négocie le meilleur duplex et la meilleure vitesse avec l'interface à l'autre extrémité du câble, mais vous pouvez forcer un duplex ou une vitesse spécifique si nécessaire. Les options répertoriées sont uniquement celles prises en charge par l'interface. Avant de définir ces options pour les interfaces sur un module de réseau, veuillez lire Limites de la configuration de l'interface, à la page 255.

- **Conditions de duplex**— Choisissez **Auto (automatique)** , **Half (demi)** ou **Full (complet)**. Les interfaces SFP prennent uniquement en charge les conditions de duplex **full (complètes)**.
- **Speed**(vitesse) : les options exactes dépendent du modèle et du type d'interface. Choisissez une vitesse, **Auto**, **No Negotiate** .le paramètre**No Negotiate** définit la vitesse à 1000 Mbit/s et désactive la négociation de liaison pour les paramètres de contrôle de flux et les informations sur les défaillances à distance.

Étape 8 Modifiez les paramètres **IPv6 Configuration**.

- **Enable DHCP for IPv6 address configuration (Activer DHCP pour la configuration d'adresse IPv6)** : pour définir l'indicateur de configuration d'adresse gérée dans le paquet de publication de routeur IPv6. Cet indicateur signale aux clients d'autoconfiguration IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des adresses, en plus de l'adresse d'autoconfiguration sans état dérivée.
- **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.
- **DAD Attempts** (tentatives de DAD) : La fréquence à laquelle l'interface effectue la détection d'adresses en double (DAD) est de 0 à 600. La valeur par défaut est 1. Pendant le processus d'autoconfiguration sans état, DAD vérifie le caractère unique des nouvelles adresses IPv6 monodiffusion avant que les adresses ne soient affectées aux interfaces. 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. L'interface utilise des messages de sollicitation de voisin pour effectuer la détection des adresses en double. Définissez la valeur sur 0 pour désactiver le traitement de la détection d'adresses en double (DAD).

Étape 9 (Facultatif, recommandé pour les sous-interfaces et les unités à haute accessibilité.) Configurez l'adresse MAC

Par défaut, le système utilise l'adresse MAC gravée dans la carte d'interface réseau (NIC) pour l'interface. Ainsi, toutes les sous-interfaces d'une interface utilisent la même adresse MAC. Vous pouvez donc créer des adresses uniques par sous-interface. Des adresses MAC actives/en attente configurées manuellement sont également recommandées si vous configurez la haute accessibilité. La définition des adresses MAC permet de maintenir la cohérence du réseau en cas de basculement.

- **MAC Address** : Le contrôle d'accès au support est au format H.H.H., où H est une valeur hexadécimale de 16 bits. Par exemple, vous devez entrer l'adresse MAC 00-0C-F1-42-4C-DE comme 000C.F142.4CDE. L'adresse MAC ne doit pas avoir le bit de multidiffusion activé; autrement dit, le deuxième chiffre hexadécimal à partir de la gauche ne peut pas être un nombre impair.
- **Standby MAC Address** (adresse MAC en veille) : À utiliser avec la haute disponibilité. 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 10 Cliquez sur **OK**.

Analyser les modifications d'interface et migrer une interface

Lorsque vous modifiez des interfaces sur le périphérique, le périphérique informe le FDM qu'une modification a eu lieu. Vous ne pourrez pas déployer votre configuration avant d'avoir effectué une analyse d'interface. Le FDM prend en charge la migration d'une interface de votre politique de sécurité vers une autre interface, donc la suppression d'une interface peut être presque transparente.

À propos de l'analyse et de la migration des interfaces

Analyse en cours :

Lorsque vous modifiez des interfaces sur le périphérique, le périphérique informe le FDM qu'une modification a eu lieu. Vous ne pourrez pas déployer votre configuration avant d'avoir effectué une analyse d'interface. Après une analyse, qui détecte toutes les interfaces ajoutées, supprimées ou restaurées, vous pouvez déployer votre configuration; cependant, les parties de la configuration qui font référence à des interfaces supprimées ne seront pas déployées.

Les modifications d'interfaces qui nécessitent une analyse comprennent l'ajout ou la suppression d'interfaces. Par exemple : changement de module réseau ; changement de l'interface allouée sur le châssis Firepower 4100/9300 ; changement d'interface sur le FTDv.

Les modifications suivantes ne bloquent pas le déploiement après une analyse :

- Appartenance à une zone de sécurité
- Appartenance à une interface EtherChannel
- Appartenance au port de commutation de l'interface VLAN Firepower 1010
- Appartenance à une interface de groupe de ponts, pour les politiques qui font référence aux BVI

Remarque Une modification de l'interface de sortie du serveur syslog ne bloquera pas le déploiement, bien que vous deviez corriger la configuration du serveur syslog, manuellement ou à l'aide de la fonction de remplacement d'interface.

Migration en cours

L'ajout d'une nouvelle interface ou la suppression d'une interface inutilisée a une incidence minime sur la configuration Firepower Threat Defense. Cependant, la suppression d'une interface utilisée dans votre politique de sécurité aura une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration Firepower Threat Defense, notamment les zones de sécurité, la NAT, le VPN, le serveur DHCP, etc.

Gestionnaire de périphériques de pare-feu prend en charge la migration d'une interface de votre politique de sécurité vers une autre interface, afin que la suppression d'une interface puisse être presque transparente.

Remarque La fonctionnalité de migration ne copie *pas* le nom, l'adresse IP et les autres paramètres de configuration d'une interface à une autre ; au lieu de cela, cette fonctionnalité modifie la politique de sécurité pour faire référence à la nouvelle interface plutôt qu'à l'ancienne interface. Vous devez configurer manuellement les nouveaux paramètres d'interface avant la migration.

Si vous devez supprimer une interface, nous vous recommandons d'ajouter la nouvelle interface et de migrer l'ancienne interface *avant* de la supprimer. Si vous ajoutez et supprimez des interfaces en même temps, le processus de migration fonctionnera toujours ; cependant, vous ne pouvez pas modifier *manuellement* les interfaces supprimées ni les politiques qui y font référence, de sorte qu'il peut être plus simple d'effectuer la migration par étapes.

Si vous remplacez une interface par une interface du même type (par exemple, vous devez effectuer une RMA sur un module réseau), vous pouvez procéder comme suit : 1. Retirez l'ancien module du châssis ; 2. Effectuez une analyse ; 3. Déployez les modifications sans rapport avec les interfaces supprimées ; 4. Remplacez le module ; 5. Effectuez une nouvelle analyse ; 6. Déployez votre configuration, y compris toutes les modifications liées aux interfaces. Vous n'avez pas besoin d'effectuer une migration si la nouvelle interface a le même identifiant d'interface et les mêmes caractéristiques que l'ancienne interface.

Lignes directrices et limites pour l'analyse et la migration d'interfaces

Migrations d'interface non prises en charge

- Interface physique vers BVI
- Interface passive vers l'interface de pare-feu
- Membres du groupe de pont
- Membres de l'interface EtherChannel
- Membres du contournement matériel ISA 3000
- Interfaces VLAN ou ports de commutation Cisco Secure Firewall 1010
- Interface de diagnostic

- Basculement et liens d'état HA
- Migration d'interfaces de différents types, par exemple la migration d'une interface de groupe de ponts vers une fonctionnalité nécessitant une interface physique

Directives supplémentaires

- Si vous devez supprimer une interface, nous vous recommandons d'ajouter la nouvelle interface et de migrer l'ancienne interface *avant* de la supprimer.
- Pour FTDv, ajoutez et supprimez des interfaces uniquement à la fin de la liste des interfaces. Si vous ajoutez ou supprimez une interface ailleurs, l'hyperviseur renumérotera vos interfaces, de sorte que les ID d'interface dans votre configuration s'alignent sur les mauvaises interfaces.
- Si une analyse ou une migration se passe mal, restaurez les interfaces d'origine sur le châssis et réanalysez pour revenir à l'état d'origine.
- Pour les sauvegardes, veillez à créer une nouvelle sauvegarde avec les nouvelles interfaces. Une restauration avec l'ancienne configuration restaurera les informations d'interface d'origine, et vous devrez refaire l'analyse/le remplacement.
- Pour la haute disponibilité, apportez les mêmes modifications d'interface sur les deux unités avant d'effectuer l'analyse d'interface sur l'unité active. Il vous suffit d'effectuer l'analyse ou la migration sur l'unité active. Les modifications de configuration sont répliquées sur l'unité de secours.

Analyser et migrer les interfaces

Analyser les modifications d'interface dans Gestionnaire de périphériques de pare-feu, et migrer les configurations d'interface à partir des interfaces supprimées. Si vous souhaitez uniquement migrer une configuration d'interface (et qu'aucune analyse n'est requise), ignorez les étapes de la procédure suivante relatives à l'analyse.



Remarque La fonctionnalité de migration ne copie *pas* le nom, l'adresse IP et les autres paramètres de configuration d'une interface à une autre ; au lieu de cela, cette fonctionnalité modifie la politique de sécurité pour faire référence à la nouvelle interface plutôt qu'à l'ancienne interface. Vous devez configurer manuellement les nouveaux paramètres d'interface avant la migration.

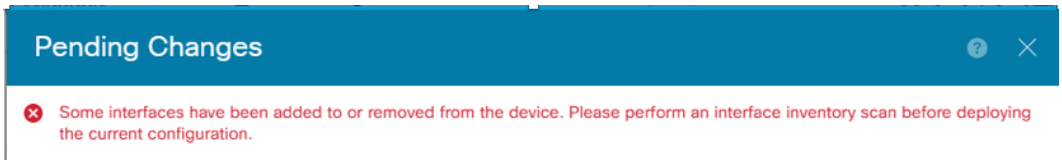
Procédure

Étape 1 Ajouter ou supprimer des interfaces sur le châssis.

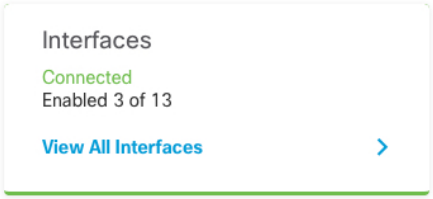
Si vous devez supprimer une interface, nous vous recommandons d'ajouter la nouvelle interface et d'effectuer un remplacement de l'ancienne interface *avant* de la supprimer.

Étape 2 Analyser les modifications d'interface.

Vous ne pourrez pas déployer votre configuration avant d'avoir effectué une analyse d'interface. Si vous essayez d'effectuer le déploiement avant une analyse, l'erreur suivante s'affiche :

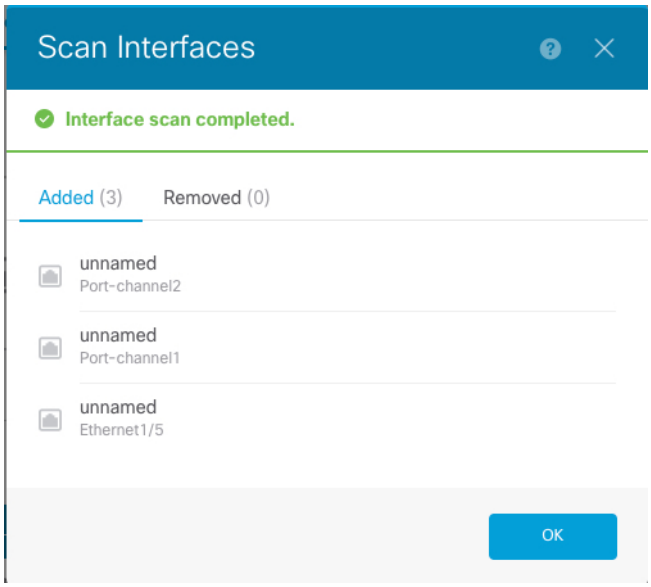


a) Cliquez sur **Device** (Périphériques), puis sur le lien **View All Interfaces** (Afficher toutes les interfaces) du résumé **Interfaces**.

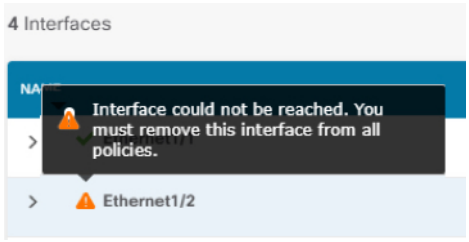


b) Cliquez sur l'icône Scan Interfaces (Analyser les interfaces) ( ).

c) Attendez que les interfaces effectuent l'analyse, puis cliquez sur **OK**.



Après l'analyse, les interfaces supprimées s'affichent sur la page Interfaces avec des symboles d'avertissement :



Étape 3 Pour migrer une interface existante vers une nouvelle interface :

a) Configurez la nouvelle interface avec un nom, une adresse IP, etc.

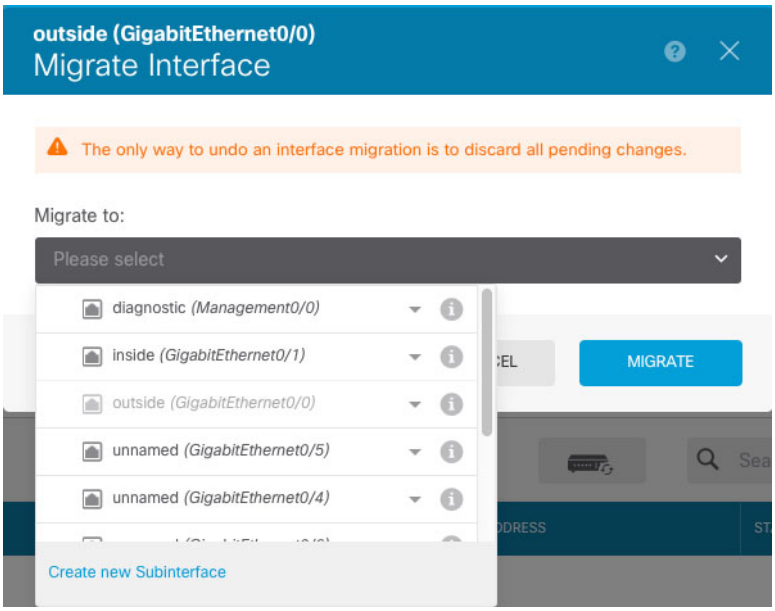
Si vous souhaitez utiliser l'adresse IP existante et le nom d'une interface que vous souhaitez supprimer, vous devez reconfigurer l'ancienne interface avec un nom et une adresse IP fictifs afin de pouvoir utiliser ces paramètres sur la nouvelle interface.

b) Cliquez sur l'icône Migrate (Migration) pour l'ancienne interface.

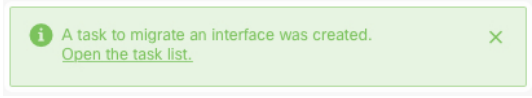


Ce processus remplace l'ancienne interface par la nouvelle interface dans tous les paramètres de configuration qui font référence à l'interface.

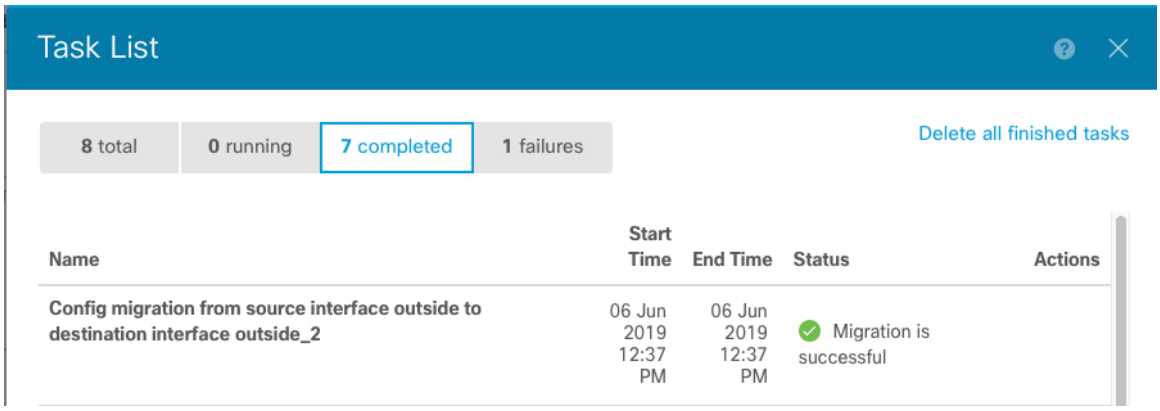
c) Choisissez la nouvelle interface dans la liste déroulante **Migrate to: (Migrer vers :)**.



d) Un message s'affiche sur la page **Interfaces**. Cliquez sur le lien dans le message.



e) Vérifiez la **liste des tâches** pour vous assurer que la migration a réussi.

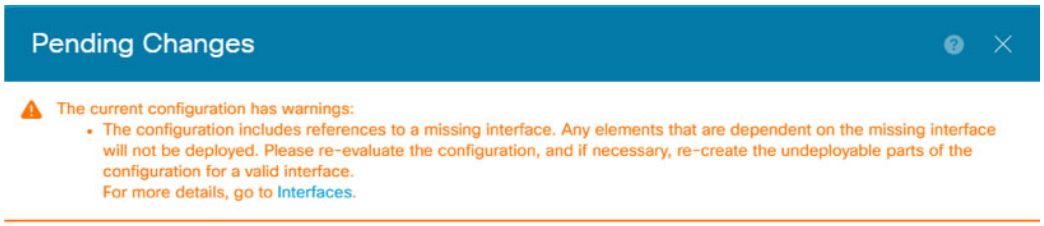


f) Si la migration échoue, vous pouvez en afficher les raisons dans API Explorer (Explorateur d'API).

Pour ouvrir l'API Explorer, cliquez sur le bouton des autres options (⋮) et choisissez **API Explorer** (Explorateur d'interface de protocole d'application). Choisissez **Interface** > **GET /jobs/interfacemigrations**, puis cliquez sur**Try it Out! (Essayez-le !)**.

Étape 4 Déployez votre configuration.

Les parties de la configuration qui font référence à des interfaces supprimées ne seront pas déployées, auquel cas vous verrez le message suivant :



Étape 5 Supprimez les anciennes interfaces du châssis, et effectuez une autre analyse.

Les interfaces supprimées qui ne sont plus utilisées dans votre politique seront supprimées de la page **Interfaces**.

Étape 6 Redéployez votre configuration pour supprimer les interfaces inutilisées de votre configuration.

Configurer le contournement matériel automatique en cas de panne de courant (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. 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. Par défaut, le contournement matériel est activé pour les deux paires d'interfaces si elles sont prises en charge.

Lorsque le contournement matériel est actif, le trafic passe entre ces paires d'interfaces au niveau de la couche 1. L'interface de ligne de commande de FTD verra les interfaces comme étant en panne.Gestionnaire de

périphériques de pare-feu Firewall Threat Defense Aucune fonction de pare-feu n'est en place, assurez-vous donc de comprendre les risques de laisser le trafic passer par le périphérique.

Nous vous suggérons de désactiver l'aléatoire des numéros de séquence TCP (comme décrit dans cette procédure). 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. La session TCP doit donc être rétablie. Même lorsque la répartition aléatoire des numéros de séquence TCP est désactivée, certaines connexions TCP devront être rétablies car la liaison a été temporairement interrompue pendant le basculement.

Dans la console de l'interface de ligne de commande ou dans une session SSH, utilisez la commande **show hardware-bypass** pour surveiller l'état opérationnel.

Avant de commencer

Pour que le contournement matériel fonctionne :

- Vous devez placer les paires d'interfaces dans le même groupe de ponts.
- Vous devez connecter les interfaces pour accéder aux ports du commutateur. Ne les connectez pas aux ports de ligne principale.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé des Interfaces.

La section **Hardware Bypass** (Contournement matériel) en haut de la page, affiche la configuration actuelle des paires d'interfaces autorisées pour ce périphérique.

Cependant, vous devez vous assurer que les paires sont configurées dans le même groupe de ponts avant de pouvoir activer le contournement matériel.

Étape 2 Cliquez sur **Edit** (Modifier) pour configurer le contournement matériel.

La boîte de dialogue **Hardware Bypass Configuration** (Configuration du contournement matériel) s'affiche.

Étape 3 Pour configurer le comportement de contournement matériel automatique, choisissez, pour chaque paire d'interfaces, l'une des options suivantes dans la zone **Hardware Bypass during Power Down** (Contournement matériel pendant la mise hors tension).

- **Disable** (Désactiver) : désactive le contournement matériel. Le trafic ne passera pas par l'appareil en cas de panne de courant.
- **Enable** (Activer) : active le contournement matériel en cas de panne de courant. Le contournement matériel garantit que le trafic n'est pas interrompu en cas de panne de courant. Notez que le trafic contourné n'est pas inspecté et que les politiques de sécurité ne sont pas appliquées. Après le rétablissement de l'alimentation, le contournement matériel est automatiquement désactivé pour que le trafic puisse circuler normalement, avec inspection. Il peut y avoir une brève interruption du trafic lorsque le contournement matériel est désactivé.
- **Enable with Persistence** (Activer avec persistance) : active le contournement matériel en cas de panne de courant et le maintient activé après le rétablissement de l'alimentation. Une fois le courant rétabli, vous devez désactiver le contournement matériel à l'aide du curseur **Manual Hardware Bypass**

(Contournement matériel manuel). Cette option vous permet de contrôler le moment de la brève interruption du trafic.

Étape 4 (Facultatif) Pour activer ou désactiver manuellement le contournement matériel, cliquez sur le curseur **Manual Hardware Bypass** (Contournement matériel manuel).

Par exemple, vous pourriez vouloir tester le système ou contourner temporairement le périphérique pour une raison quelconque. Notez que vous devez déployer la configuration pour modifier l'état du contournement matériel; la simple modification des paramètres n'est pas suffisante.

Lorsque vous activez ou désactivez manuellement le contournement matériel, vous verrez les messages de journal système suivants, où *pair* est 1/1-1/2 ou 1/3-1/4.

- %FTD-6-803002 : aucune protection ne sera fournie par le système pour le trafic sur GigabitEthernet *pair*
- %FTD-6-803003 : l'utilisateur a désactivé le contournement manuel sur GigabitEthernet *pair*

Étape 5 Cliquez sur **OK**.

La modification n'est pas immédiate. Vous devez déployer la configuration.

Étape 6 (Facultatif) Créez l'objet FlexConfig et la politique nécessaires pour désactiver la aléatoireisation du numéro de séquence TCP.

a) Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

b) Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

c) Cliquez sur le bouton **+** pour créer un nouvel objet.

d) Saisissez un nom pour l'objet. Par exemple, **Disable_TCP_Randomization**.

e) Dans l'éditeur **Template** (Modèle), saisissez les commandes permettant de désactiver la randomisation du numéro de séquence TCP.

La commande est **set connection random-sequence-number disable**, mais vous devez la configurer pour une classe spécifique dans une carte de politique. De loin, l'approche la plus simple est de désactiver les numéros de séquence aléatoires globalement, ce qui nécessite les commandes suivantes :

```
policy-map global_policy
 class default_class
  set connection random-sequence-number disable
```

f) Dans l'éditeur **Negate Template** (Modèle d'annulation), saisissez les lignes nécessaires pour annuler cette configuration.

Par exemple, si vous désactivez la randomisation du numéro de séquence TCP globalement, le modèle d'annulation serait le suivant :

```
policy-map global_policy
 class default_class
  set connection random-sequence-number enable
```

g) Cliquez sur **OK** pour enregistrer l'objet.

Vous devez maintenant ajouter l'objet à FlexConfig Policy (politique FlexConfig). La création de l'objet n'est pas suffisante.

h) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières.
i) Cliquez sur + dans la liste des groupes.
j) Sélectionnez l'objet Disable_TCP_RandOMization et cliquez sur **OK**.

   L'aperçu doit être mis à jour avec les commandes du modèle. Vérifiez que vous voyez les commandes attendues.

k) Cliquez sur **Save** (enregistrer).

   Vous pouvez maintenant déployer la politique.

Surveillance des interfaces

Vous pouvez afficher des renseignements de base sur les interfaces dans les zones suivantes :

- **Device** (Périphérique). Utilisez le graphique de port pour surveiller l'état actuel des interfaces. Passez le curseur sur un port pour voir ses adresses IP, l'appartenance à EtherChannel et les états d'activation et de liaison. Les adresses IP peuvent être attribuées statiquement ou obtenues à l'aide de DHCP.

  Les ports d'interface utilisent le code de couleur suivant :

  - Vert — l'interface est configurée, activée et la liaison est activée.
  - Gris — l'interface n'est pas activée.
  - Orange/rouge — l'interface est configurée et activée, mais la liaison est en panne. Si l'interface est câblée, il s'agit d'une condition d'erreur qui doit être corrigée. Si l'interface n'est pas câblée, il s'agit de l'état attendu.

- **Monitoring (Surveillance)** > **System (Système)**. Le tableau de bord **Throughput** (Débit) affiche des informations sur le trafic circulant dans le système. Vous pouvez afficher les informations sur toutes les interfaces ou sélectionner une interface spécifique à examiner.
- **Monitoring (Surveillance)** > **Zones**. Ce tableau de bord affiche les statistiques en fonction des zones de sécurité, qui sont composées d'interfaces. Vous pouvez explorer ces informations pour plus de détails.

Surveillance des interfaces dans l'interface de ligne de commande

Vous pouvez également ouvrir la console CLI ou vous connecter à l'interface de ligne de commande du périphérique et utiliser les commandes suivantes pour obtenir des informations plus détaillées sur le comportement et les statistiques liés à l'interface.

- **show interface** affiche les informations de configuration et d'état de l'interface. Cette commande comporte de nombreux mots-clés que vous pouvez utiliser pour obtenir les informations dont vous avez besoin. Utilisez ? en tant que mot-clé pour voir les options disponibles.
- **show ipv6 interface** affiche les informations de configuration IPv6 des interfaces.
- **show bridge-group** affiche les informations sur les interfaces virtuelles de pont (BVI), y compris les informations sur les membres et les adresses IP.
- **show conn** affiche les informations sur les connexions actuellement établies par les interfaces.

- **show traffic** affiche les statistiques sur le trafic circulant dans chaque interface.
- **show ipv6 traffic** affiche les statistiques sur le trafic IPv6 circulant dans le périphérique.
- **show dhcpd** affiche les statistiques et d'autres informations sur l'utilisation de DHCP sur les interfaces, en particulier sur les serveurs DHCP configurés sur les interfaces.
- **show switch vlan** affiche l'association VLAN-port de commutation.
- **show switch mac-address-table** affiche les entrées d'adresses MAC statiques et dynamiques.
- **show arp** affiche les entrées d'ARP dynamiques, statiques et de serveur mandataire.
- **show power inline** affiche l'état PoE.
- **show vpdn group** affiche les groupes PPPoE ainsi que les noms d'utilisateurs et l'authentification configurés.
- **show vpdn username** affiche les noms d'utilisateur et les mots de passe PPPoE.
- **show vpdn session pppoe state** affiche l'état de la session PPPoE.

Exemples d'interfaces

Le chapitre de scénarios d'utilisation comprend les exemples liés aux interfaces suivants :

- Comment configurer l'appareil en FDM, à la page 43
- Comment ajouter un sous-réseau, à la page 73
- Comment surveiller passivement le trafic sur un réseau, à la page 78



PARTIE IV

Routage

- Bases de routage et routes statiques, à la page 315
- Routeurs virtuels, à la page 333
- Cartes de routage et autres objets pour le réglage du routage , à la page 359
- Open Shortest Path First (OSPF), à la page 379
- Protocole de routage de passerelle intérieure amélioré (EIGRP), à la page 401
- Protocole de routage BGP, à la page 419



CHAPITRE 12

Bases de routage et routes statiques

Le système utilise une table de routage pour déterminer l'interface de sortie des paquets qui entrent dans le système. Les rubriques suivantes expliquent les bases du routage et comment configurer le routage statique sur le périphérique.

- Bonnes pratiques pour le routage, à la page 315
- Aperçu du routage, à la page 315
- Routes statiques, à la page 322
- Surveillance du routage, à la page 330

Bonnes pratiques pour le routage

La conception des processus de routage dans un réseau peut être un processus complexe. Ce chapitre suppose que vous configurez le périphérique Firepower Threat Defense pour qu'il fonctionne dans un réseau existant et qu'il participe aux processus de routage que vous avez déjà établis dans ce réseau.

Si vous créez plutôt un nouveau réseau, prenez le temps de vous renseigner ailleurs sur les protocoles de routage et sur la façon de concevoir un plan de routage efficace adapté à votre réseau. Ce chapitre ne présente pas de recommandations pour le choix des protocoles et ne détaille pas non plus leur fonctionnement.

Si votre réseau est très petit et que vous vous connectez simplement à un fournisseur de services Internet, vous n'aurez peut-être besoin que de quelques routes statiques et vous n'aurez peut-être pas du tout besoin de mettre en œuvre des protocoles de routage.

Mais si vous configurez un grand réseau qui inclura de nombreux routeurs, vous devrez probablement mettre en œuvre au moins un protocole de routage pour le routage interne, comme OSPF, et possiblement un autre pour le routage externe, comme BGP. Votre fournisseur de services peut vous aider à comprendre quel routage externe pourrait être nécessaire, le cas échéant. S'il s'agit de votre situation, commencez par déterminer quels protocoles de routage vous pouvez configurer à l'aide de Firepower Threat Defense, puis planifiez votre réseau et, enfin, configurez le périphérique Firepower Threat Defense en fonction de ce plan.

Aperçu du routage

Les rubriques suivantes décrivent le comportement du routage dans le périphérique Firepower Threat Defense. Le routage est l'action de déplacer des informations sur un réseau d'une source à une destination. En cours de route, au moins un nœud intermédiaire est généralement rencontré. Le routage comporte deux activités de base : la détermination des chemins de routage optimaux et le transport de paquets dans un réseau.

Protocoles de routage pris en charge

Le tableau suivant explique les protocoles de routage et les technologies que vous pouvez configurer sur un périphérique Firewall Threat Defense à l'aide de Gestionnaire de périphériques de pare-feu, ainsi que la méthode que vous devez utiliser pour terminer la configuration.

Tableau 9 : Protocoles de routage pris en charge

Fonctionnalités de routage	Méthode de configuration	Notes
BGP	Smart CLI	Configurez les objets d'interface de ligne de commande BGP à partir de la page **Device (Périphérique)** > **Routing (Routage)**. Configurez les objets utilisés dans BGP, tels que les cartes de routage, à l'aide d'objets Smart CLI à partir de la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
Détection de transfert bidirectionnel (BFD)	FlexConfig	Configurez BFD à l'aide d'objets FlexConfig à partir de la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**. BFD est pris en charge uniquement avec BGP.
EIGRP	Smart CLI	Configurez les objets d'interface de ligne de commande Smart EIGRP à partir de la page **Device (Périphérique)** > **Routing (Routage)**. Configurez les objets utilisés dans EIGRP, comme les route maps, à l'aide d'objets Smart CLI depuis la page**Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
IS-IS	FlexConfig	Configurez IS-IS à l'aide d'objets FlexConfig à partir de la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
Routage multidiffusion	FlexConfig	Configurez le routage multidiffusion à l'aide d'objets FlexConfig depuis la page**Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
OSPFv2	Smart CLI	Configurez les objets Smart CLI OSPFv2 à partir de la page **Device (Périphérique)** > **Routing (Routage)**. Configurez les objets utilisés dans OSPFv2, comme les route maps, à l'aide d'objets Smart CLI depuis la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
OSPFv3	—	La configuration OSPFv3 n'est pas prise en charge.
Routage à base de règles (PBR)	FlexConfig	Configurez le routage à base de règles (PBR) à l'aide d'objets FlexConfig depuis la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Fonctionnalités de routage	Méthode de configuration	Notes
RIP	FlexConfig	Configurez le protocole RIP à l'aide des objets FlexConfig à partir de la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
du routage statique;	Gestionnaire de périphériques de pare-feu	Configurez les routes statiques globalement ou par routeur virtuel à partir de la page **Device (Périphérique)** > **Routing (Routage)**.
Routeurs virtuels, VRF	Gestionnaire de périphériques de pare-feu	Configurez les routeurs virtuels à partir de la page **Device (Périphérique)** > **Routing (Routage)**.

Types de route

Il existe deux types principaux de routage : statique ou dynamique.

Les routes statiques sont celles que vous définissez explicitement. Il s'agit de routes stables, normalement de priorité élevée, que vous utiliseriez pour vous assurer que le trafic vers la destination de route est toujours envoyé par la bonne interface. Par exemple, vous créeriez une route statique par défaut pour couvrir tout le trafic qui n'est déjà couvert par aucune autre route, c'est-à-dire 0.0.0.0/0 pour IPv4 ou ::/0 pour IPv6. Un autre exemple serait une route statique vers un serveur syslog interne que vous souhaitez toujours utiliser.

Les routes dynamiques sont celles apprises par l'application d'un protocole de routage, tel que OSPF, BGP, EIGRP, IS-IS ou RIP. Vous ne définissez pas les routes directement. Au lieu de cela, vous configurez le protocole de routage, et le système communique ensuite avec les routeurs voisins, en leur transmettant les mises à jour de routage et en recevant les mises à jour de routage.

Les protocoles de routage dynamique ajustent la table de routage 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 système recalcule les routes 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.

Le routage statique est simple et sert le routage de base. Il fonctionne bien dans des environnements où le trafic réseau est relativement prévisible et où la conception de réseau est relativement simple. Cependant, comme les routes statiques ne peuvent pas changer à moins que vous ne les modifiez, elles ne peuvent pas réagir aux modifications dans le réseau.

Sauf si vous avez un petit réseau, vous combinez généralement des routes statiques avec un ou plusieurs protocoles de routage dynamique. Vous définissez au moins une route statique, comme route par défaut pour tout trafic qui ne correspond pas à une route explicite.



Remarque Vous pouvez utiliser l'interface de ligne de commande Smart pour configurer les protocoles de routage suivants : OSPF, BGP. Utilisez FlexConfig pour configurer d'autres protocoles de routage pris en charge dans le logiciel ASA.

La table de routage et la sélection de route

Lorsque les traductions (xlates) et les règles NAT ne déterminent pas l'interface de sortie, le système utilise la table de routage pour déterminer le chemin d'un paquet.

Les routes dans la table de routage comprennent une métrique appelée « distance administrative » qui fournit une priorité relative à une route donnée. Si un paquet correspond à plus d'une entrée de route, celle ayant la distance la plus faible est utilisée. Les réseaux directement connectés (ceux définis sur une interface) ont la distance 0, ils sont donc toujours privilégiés. Les routes statiques ont une distance par défaut de 1, mais vous pouvez les créer avec n'importe quelle distance comprise entre 1 et 254.

Les routes qui identifient une destination spécifique prévalent sur la route par défaut (la route dont la destination est 0.0.0.0/0 ou ::/0).

Mode de remplissage de la table de routage

La table de routage FTD 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 FTD 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 FTD 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 FTD 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 Appareil FTD 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 Appareil FTD.

Tableau 10 : 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
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' Appareil FTD 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' Appareil FTD 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' Appareil FTD 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' Appareil FTD 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 Appareil FTD. 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.

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 FTD 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 du tableau de gestion uniquement en provenance du périphérique comprend les communications du serveur AAA.
- Le trafic du tableau de données du périphérique comprend les recherches de serveur DNS et le DDNS. Une exception est que si vous spécifiez uniquement l'interface de diagnostic pour DNS, le périphérique Firewall Threat Defense utilisera uniquement le tableau de gestion uniquement.

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.

Remarque L'interface virtuelle de gestion utilise sa propre table de routage Linux qui ne fait pas partie de la recherche de routage Firewall Threat Defense. Le trafic provenant de l'interface de gestion comprend les sessions de gestion Gestionnaire de périphériques de pare-feu, la communication des licences et les mises à niveau de la base de données. L'interface logique de diagnostic, quant à elle, utilise la table de routage de gestion uniquement décrite dans cette section.

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 FTD vérifiera uniquement les routes pour l'interface spécifiée. Par exemple, si vous devez communiquer avec un serveur RADIUS sur une interface de données, spécifiez cette interface dans la configuration RADIUS. Sinon, s'il existe une route par défaut dans la table de routage de gestion uniquement, elle correspondra à la route par défaut et ne reviendra jamais à la table de routage des données.

Routage à chemins multiples à coûts égaux (ECMP)

L' Appareil FTD 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' Appareil FTD 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.

Routes statiques

Vous pouvez créer des routes statiques pour fournir un routage de base à votre réseau.

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 Appareil FTD 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 FTD 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. L'interface de dépistage est incluse dans le tableau des valeurs de gestion uniquement. L'interface de gestion spéciale utilise une table de routage Linux distincte et possède sa propre voie 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 Appareil FTD.
- Vous utilisez une fonctionnalité qui ne prend pas en charge les protocoles de routage dynamique.

Routes statiques de sauvegarde et suivi de 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 tombe en panne.

En mettant en œuvre le suivi de routage, à l'aide d'un moniteur de contrat de niveau de service (SLA), vous pouvez suivre la disponibilité d'un routage statique et installer automatiquement un routage de secours en cas de défaillance du routage principal. 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.

Lorsque vous utilisez le suivi de routage, vous associez une adresse IP cible sur le réseau de destination au routage suivi. Le système utilise ensuite les requêtes d'écho ICMP pour vérifier périodiquement que l'adresse est accessible. Si le système ne reçoit pas de réponse d'écho dans le délai que vous spécifiez, l'hôte est estimé comme inaccessible et le système supprime la route associée de la table de routage. Le système peut alors utiliser une route de secours non suivie avec une mesure plus élevée à la place de la route supprimée.

Ainsi, pour utiliser une route statique de secours pour une destination donnée, y compris pour une route par défaut, vous devez procéder comme suit :

1. Créez un moniteur SLA qui surveillera une adresse IP fiable sur le réseau de destination, comme une passerelle ou un serveur permanent (comme un serveur Web ou un serveur Syslog). Ne surveillez pas l'adresse IP d'un système qui pourrait être mis hors ligne alors que le réseau de destination reste sain et disponible. Consultez Configurer les objets du moniteur SLA, à la page 326.
2. Créez la route principale vers la destination et sélectionnez le moniteur SLA pour la route. La métrique pour cette route doit généralement être 1. Consultez Configuration des routes statiques, à la page 325.

3. Créez la route statique de secours qui sera utilisée en cas de défaillance de la route principale. Cette route doit avoir une métrique plus grande que la route principale. Par exemple, si la route principale est 1, la route de secours pourrait être 10. Vous devez également normalement sélectionner une interface différente pour la route de secours.

Lignes directrices relatives au routage statique

Groupes de ponts

- En mode routé, vous devez spécifier les BVI comme passerelle; vous ne pouvez pas définir l'interface membre.
- Pour le trafic qui provient de l' Appareil FTD (comme syslog ou SNMP) et qui doit traverser une interface membre d'un groupe de ponts vers un réseau non directement connecté, vous devez configurer soit une route par défaut, soit des routes statiques, afin que l' Appareil FTD sache par quelle interface membre du groupe de ponts envoyer le trafic. Si certains serveurs ne peuvent pas être atteints par une seule route par défaut, vous devez configurer des routes statiques.
- Le suivi de routage statique n'est pas pris en charge pour les interfaces membres des groupes de ponts ou sur les BVI.

IPv6

- Le suivi de routage statique (surveillance SLA) n'est pas pris en charge pour IPv6.

Zones de trafic à chemins multiples (ECMP) à coût égal

- Conservez les interfaces membres d'une zone de trafic ECMP dans la même zone de sécurité pour éviter que différentes critères d'accès, SSL ou d'identité ne soient appliquées à ces interfaces.
- Vous pouvez avoir jusqu'à 8 routes à coût égal pour un réseau dans une zone de trafic ECMP donnée.
- Vous pouvez créer jusqu'à 256 zones de trafic ECMP, avec jusqu'à 8 interfaces par zone.
- Les zones de trafic ECMP peuvent contenir des interfaces physiques, des sous-interfaces et des EtherChannels nommés. Elles ne peuvent pas contenir les éléments suivants :
  - Un groupe de ponts (BVI) ou ses membres
  - Interfaces membre EtherChannel
  - Interfaces HA (basculement ou liaisons d'état)
  - Interfaces de gestion uniquement
  - Interfaces utilisées pour les connexions VPN de site à site ou VPN d'accès à distance.
  - Interfaces de tunnel virtuel (VTI) ou leurs interfaces source.
  - Interfaces configurées pour l'accès de gestion VPN.
- Vous ne pouvez pas activer le relais DHCP sur une interface dans une zone.

Configuration des routes statiques

Définissez des routes statiques pour indiquer au système où envoyer les paquets qui ne sont pas liés aux réseaux directement connectés aux interfaces du système.

Vous avez besoin d'au moins une route statique, la route par défaut, pour le réseau 0.0.0.0/0. Cette route définit où envoyer les paquets dont l'interface de sortie ne peut pas être déterminée par les xlates NAT existants (traductions) ou les règles NAT statiques, ou d'autres routage statiques.

Vous pourriez avoir besoin d'autres routages statiques si la passerelle par défaut ne peut pas être utilisée pour accéder à tous les réseaux. Par exemple, le routeur par défaut est généralement un routeur en amont sur l'interface externe. S'il existe d'autres réseaux internes qui ne sont pas directement connectés au périphérique et qu'ils ne sont pas accessibles au moyen de la passerelle par défaut, vous avez besoin de routages statiques pour chacun de ces réseaux internes.

Vous ne pouvez pas définir de routages statique pour les réseaux qui sont directement connectés aux interfaces du système. Le système crée automatiquement ces routes.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis cliquez sur le lien dans le sommaire de **Routing (routage)**.

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez une route statique.

Étape 3 Sur la page de **routage statique**, effectuez l'une des opérations suivantes :

- Pour ajouter une nouvelle route, cliquez sur **+**.
- Cliquez sur l'icône de modification ( ) de la route que vous souhaitez modifier.

Si vous n'avez plus besoin d'un routage, cliquez sur l'icône de la corbeille pour le supprimer.

Étape 4 Configurer les propriétés du routage

- **Name (nom)** : nom d'affichage du routage.
- **Description** : une description facultative de l'objectif du routage.
- **Interface** : sélectionnez l'interface par laquelle vous souhaitez envoyer le trafic. L'adresse de la passerelle doit être accessible au moyen de cette interface.

  Pour les groupes de pontage, vous configurez la route pour l'interface de groupe de pontage (BVI), pas pour les interfaces membres.

  Si vous avez activé le routage et le transfert virtuels, vous pouvez sélectionner une interface qui appartient à un autre routeur virtuel. Si vous créez un routage statique dans un routeur virtuel pour une interface dans un routeur virtuel différent, la route franchira les limites du routeur virtuel, avec le risque que le trafic de ce routeur virtuel se répande dans un autre routeur virtuel. Cela peut être le résultat souhaité, mais déterminez avec soin que vous avez besoin de cette fuite de routage. Lorsque vous sélectionnez des interfaces, le nom du routeur virtuel auquel appartient l'interface s'affiche à droite de l'interface.
- **Protocol (Protocole)**— Sélectionnez si la route est pour une adresse **IPv4** or **IPv6** address.
- **Networks (réseaux)** : sélectionnez les objets réseau qui identifient les réseaux de destination ou les hôtes qui doivent utiliser la passerelle dans ce routage.

Pour définir une route par défaut, utilisez les objets réseau prédéfinis any-ipv4 ou any-ipv6, ou créez un objet pour le réseau 0.0.0.0/0 (IPv4) ou ::/0 (IPv6).

- **Passerelle** : sélectionnez l'objet réseau hôte qui identifie l'adresse IP de la passerelle. Le trafic est envoyé à cette adresse. Vous ne pouvez pas utiliser la même passerelle pour les routages sur plusieurs interfaces.

  Si vous définissez un routage dans un routeur virtuel et que l'interface appartient à un autre routeur virtuel, vous devez laisser la passerelle vide. Le système acheminera le trafic vers ces réseaux vers l'autre routeur virtuel, puis utilisera la table de routage du routeur virtuel cible pour déterminer la passerelle.

- **Métrique** : la distance administrative pour la route, entre 1 et 254. La valeur par défaut pour les routes statiques est 1. S'il y a des routeurs supplémentaires entre l'interface et la passerelle, saisissez le nombre de sauts comme distance administrative.

  La distance administrative est un paramètre utilisé pour comparer les routages. Plus le nombre est bas, plus la priorité est donnée au routage. Les routages connectés (réseaux directement connectés à une interface sur le périphérique) ont toujours la priorité sur les routages statiques.

Étape 5 (Facultatif; routages IPv4 uniquement.) Sélectionnez le **moniteur SLA** qui doit suivre la viabilité de ce routage.

Un moniteur SLA peut vérifier qu'un hôte toujours disponible sur le réseau cible est accessible. S'il devient inaccessible, le système peut installer un routage de secours. Par conséquent, si vous configurez un moniteur SLA, vous devez également configurer un autre routage statique, avec une mesure plus importante, pour ce réseau. Par exemple, si ce routage a la métrique 1, créez un routage de secours avec la métrique 10. Pour en savoir plus, consultez Routes statiques de sauvegarde et suivi de routage statique, à la page 323.

Si l'objet SLA Monitor n'existe pas encore, cliquez sur le lien **Create SLA Monitor (créez un moniteur SLA)** en bas de la liste et créez-le maintenant.

Remarque
Si un routage surveillé est supprimé parce que l'adresse surveillée ne peut pas faire l'objet d'un ping, le routage est indiqué dans la table de routage statique avec un avertissement indiquant que la route est inaccessible. Déterminez si le problème est temporaire ou si vous devez reconfigurer le routage. Envisagez la possibilité que le routage soit viable, mais que l'adresse surveillée ne soit pas suffisamment fiable.

Étape 6 Cliquez sur **OK**.

Configurer les objets du moniteur SLA

Configurer les objets du moniteur de contrat par niveau de service (SLA) pour une utilisation avec des routes statiques. À l'aide d'un moniteur SLA, vous pouvez suivre l'intégrité d'un routage statique et remplacer automatiquement un routage défaillant par un nouveau. pour obtenir plus de renseignements sur le suivi de routage, consultez Routes statiques de sauvegarde et suivi de routage statique, à la page 323.

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 quelle adresse IP, définie dans un objet réseau hôte, mais vous devriez envisager d'utiliser les éléments 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.
- Serveur sur le réseau cible, tel qu'un serveur syslog, avec lequel le système doit communiquer.

- Une adresse IP persistante sur le réseau de destination. Un poste de travail qui peut être fermé la nuit n'est pas un bon choix.

Procédure

Étape 1 Select **Objects (objets)**, then select **SLA Monitors** from the table of contents.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Définissez les options requises pour le moniteur SLA :

- **Monitor Address (adresse de surveillance)** : sélectionnez l'objet réseau hôte qui définit l'adresse à surveiller sur le réseau de destination. Vous pouvez cliquer sur **Create New Network (créer un nouveau réseau)** si l'objet dont vous avez besoin n'existe pas.

  Cette adresse est surveillée uniquement si vous connectez le moniteur SLA à une route statique.

- **Target interface interface cible)** : sélectionnez l'interface par laquelle envoyer les paquets de demande d'écho. Il s'agit normalement de l'interface sur laquelle vous allez définir la route statique. L'adresse source de l'interface est utilisée comme adresse source dans les paquets de demande d'écho.

Étape 5 (Facultatif) Ajustez les **options d'écho IP ICMP**.

Toutes les options ICMP ont des valeurs par défaut qui sont appropriées dans la plupart des cas, mais vous pouvez les régler en fonction de vos besoins.

- **Threshold (Seuil)** : le nombre de millisecondes pour qu'un seuil croissant soit déclaré, de 0 à 2147483647. La valeur par défaut est 5000 (5 secondes). Cette valeur ne doit pas être supérieure à la valeur définie pour le délai d'expiration. La valeur de seuil est uniquement utilisée pour indiquer les événements de dépassement de seuil, qui ne touchent pas l'accessibilité. Vous pouvez utiliser la fréquence des événements de seuil pour évaluer le paramètre de délai d'expiration.
- **Timeout (délai d'expiration)** : le temps, en millisecondes, pendant lequel l'opération de surveillance du routage doit attendre une réponse des paquets de demande, est compris entre 0 et 60 480 000 millisecondes (7 jours). La valeur par défaut est de 5 000 millisecondes (5 secondes). Si le moniteur ne reçoit pas de réponse à au moins une demande d'écho pendant cette période, le processus installe la route de secours.
- **Frequency (fréquence)** : le nombre de millisecondes entre les sondes SLA, de 1 000 à 60 480 000, en multiples de 1 000. Vous ne pouvez pas définir une fréquence inférieure à la valeur du délai d'expiration. La valeur par défaut est de 60 000 millisecondes (60 secondes).
- **Type of Service (type de service)** : un entier qui définit le type de service (toS) dans l'en-tête IP du paquet de requête d'écho ICMP, de 0 à 255. La valeur par défaut est 0.

- **Number of Packets (nombre de paquets)** : nombre de paquets à envoyer avec chaque interrogation, de 1 à 100. La valeur par défaut est 1 paquet.
- **Data Size (taille des données)** : taille de la charge utile de données à utiliser dans les paquets de demande d'écho, de 0 à 16 384 octets. La valeur par défaut est 28. Ce paramètre spécifie la taille de la charge utile uniquement; il ne spécifie pas la taille du paquet entier.

Étape 6 Cliquez sur **OK**.

Vous pouvez désormais utiliser l'objet moniteur SLA dans une route statique.

Configuration des zones de trafic ECMP

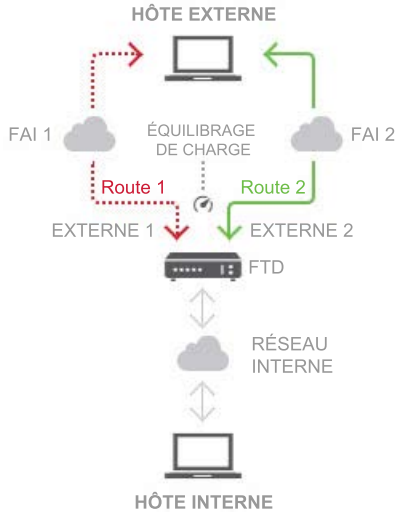
Normalement, pour configurer plusieurs routes pour un préfixe réseau donné, avec la même métrique de routage, vous devez configurer les routes sur la même interface. Ainsi, le système utilise le routage ECMP (Equal-Cost Multi-Path) pour équilibrer la charge du trafic envoyé par l'interface vers les passerelles.

Par exemple, vous pouvez configurer plusieurs routes par défaut sur l'interface externe qui spécifient différentes passerelles, et cette configuration est autorisée sans modifications supplémentaires.

```
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
```

Vous pouvez également utiliser ECMP pour équilibrer le trafic sur plusieurs interfaces (au sein d'un routeur virtuel) pour le même préfixe de réseau et la même métrique de routage. Cette configuration est nécessaire si les passerelles sont accessibles par des interfaces distinctes. Par exemple, si vous avez deux fournisseurs de services Internet et que vous souhaitez équilibrer la charge entre eux, sans diviser vos espaces d'adresses internes entre les passerelles ISP. Un fournisseur de services Internet est accessible par l'interface outside1 et l'autre par l'interface outside2. Pour ce faire, vous devez créer une zone de trafic de routage qui contient les interfaces outside1 et outside2.

```
isp-zone containing outside1 and outside2
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 10.1.1.3
```



Remarque Une zone de trafic de routage ECMP n'est pas liée aux zones de sécurité. La création d'une zone de sécurité qui contient les interfaces outside1 et outside2 ne met pas en œuvre une zone de trafic à des fins de routage ECMP.

La procédure suivante explique comment configurer les zones ECMP pour profiter du traitement ECMP sur l'ensemble des interfaces.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez une route statique.

Étape 3 Cliquez sur l'onglet **ECMP Traffic Zones** (Zones de trafic ECMP).

Étape 4 Sur la page **ECMP Traffic Zones** (Zones de trafic ECMP), effectuez l'une des opérations suivantes :

- Pour ajouter une nouvelle zone, cliquez sur **+**, ou **Add ECMP Traffic Zone** (Ajouter une zone de trafic ECMP).
- Cliquez sur l'icône de modification ( ) de la zone que vous souhaitez modifier.

Si vous n'avez plus besoin d'une zone, cliquez sur l'icône de la corbeille pour la supprimer. Vous devez supprimer toutes les routes statiques qui dépendent d'une zone avant de pouvoir supprimer la zone.

Étape 5 Entrez un **Name** (Nom) pour la zone et, facultativement, une description.

Étape 6 Sélectionnez jusqu'à 8 **Interfaces** à inclure dans la zone :

- Cliquez sur **+** pour ajouter une interface.
- Cliquez sur **x** à droite d'une interface pour la supprimer.

Lors de la sélection des interfaces, gardez les restrictions suivantes à l'esprit :

- Vous pouvez sélectionner des interfaces physiques, des sous-interfaces et des canaux EtherChannel.
- Une zone de trafic ECMP ne peut pas inclure les types d'interfaces suivants : un groupe de ponts (BVI) ou ses membres, des interfaces membres EtherChannel, des interfaces de haute disponibilité (basculement ou liens d'état), des interfaces réservées à la gestion, des interfaces de tunnel virtuel (VTI) ou des interfaces configurées pour accéder à la gestion du VPN.
- Vous ne pouvez pas inclure d'interfaces utilisées dans des connexions VPN d'accès à distance ou de site à site.
- Vous ne pouvez pas sélectionner d'interfaces activées pour le relais DHCP, que ce soit comme serveur ou comme agent.
- Les interfaces doivent être attribuées au même routeur virtuel.
- Une interface ne peut se trouver que dans une seule zone de trafic.

Étape 7 Cliquez sur **OK**.

Prochaine étape

Vous pouvez maintenant accéder à l'onglet Static Routes (Routes statiques) et créer des routes à coût égal par l'intermédiaire de ces interfaces pour la même destination. Sinon, vos protocoles de routage dynamique peuvent configurer automatiquement des routes à coût égal si elles sont distribuées dans le système.

Surveillance du routage

Pour surveiller et dépanner le routage, ouvrez la console de l'interface de ligne de commande ou connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes. Vous pouvez également sélectionner certaines de ces commandes dans le menu **Commands** (Commandes) sur la page Routing (Routage).

- **show route** affiche la table de routage des interfaces de données, y compris les routes pour les réseaux directement connectés.
- **show ipv6 route** affiche la table de routage IPv6 pour les interfaces de données, y compris les routes pour les réseaux directement connectés.
- **show network** affiche la configuration de l'interface de gestion virtuelle , y compris la passerelle de gestion. Le routage via l'interface de gestion virtuelle n'est pas géré par la table de routage de l'interface de données, sauf si vous spécifiez des interfaces de données comme passerelle de gestion.
- **show network-static-routes** affiche les routes statiques configurées pour l'interface de gestion virtuelle à l'aide de la commande **configure network static-routes** . Normalement, il n'y aura pas de routes statiques, car la passerelle de gestion est suffisante pour le routage de gestion dans la plupart des cas. Ces routes ne sont pas disponibles pour le trafic sur les interfaces de données. Cette commande n'est pas disponible dans la console d'interface de ligne de commande.
- **show ospf** affiche des informations sur les processus OSPF et les routes apprises. Utilisez **show ospf ?** pour obtenir la liste des options que vous pouvez inclure afin d'afficher des informations précises sur OSPF.

- **show bgp** affiche des informations sur les processus BGP et les routes apprises. Utilisez **show bgp ?** pour obtenir une liste d'options que vous pouvez inclure pour afficher des informations spécifiques sur BGP.
- **show eigrp** *option* affiche des informations sur les processus EIGRP et les routes apprises. Utilisez **show eigrp ?** pour obtenir une liste d'options que vous pouvez inclure ; vous devez fournir une option.
- **show isis** *option* affiche des informations sur les processus IS-IS et les routes apprises. Utilisez **show isis ?** pour obtenir une liste d'options que vous pouvez inclure; vous devez fournir une option.
- **show rip database** affiche des renseignements sur les processus RIP et les routes apprises.
- **show vrf** affiche les renseignements sur les routeurs virtuels définis sur le système.
- **show zone** affiche les informations sur les zones de trafic ECMP, y compris les interfaces qui font partie de chaque zone.



CHAPITRE 13

Routeurs virtuels

Vous pouvez créer des routeurs virtuels pour isoler le trafic sur les sous-ensembles d'interfaces les uns des autres.

- À propos des routeurs virtuels et du routage et transfert virtuel (VRF), à la page 333
- Lignes directrices pour les routeurs virtuels, à la page 336
- Gestion des routeurs virtuels, à la page 338
- Exemples pour les routeurs virtuels, à la page 342
- Surveillance des routeurs virtuels, à la page 358

À propos des routeurs virtuels et du routage et transfert virtuel (VRF)

Vous pouvez créer plusieurs routeurs virtuels afin de gérer des tables de routage distinctes pour des groupes d'interfaces. Étant donné que chaque routeur virtuel possède sa propre table de routage, vous pouvez assurer une séparation nette du trafic circulant à travers le périphérique.

Vous pouvez ainsi fournir une assistance à deux clients distincts ou plus concernant un ensemble d'équipements réseau communs. Vous pouvez également utiliser des routeurs virtuels pour renforcer la séparation entre les éléments de votre propre réseau, par exemple en isolant un réseau de développement de votre réseau d'entreprise général.

Les routeurs virtuels mettent en œuvre la version « allégée » du routage et transfert virtuel, ou VRF-Lite, qui ne prend pas en charge Multiprotocol Extensions for BGP (MBGP).

Lorsque vous créez un routeur virtuel, vous affectez des interfaces au routeur. Vous pouvez affecter une interface donnée à un seul routeur virtuel. Vous devez ensuite définir les routes statiques et configurer les protocoles de routage tels qu'OSPF ou BGP pour chaque routeur virtuel. Vous devez également configurer des processus de routage distincts sur l'ensemble de votre réseau, de sorte que les tables de routage sur tous les périphériques participants utilisent les mêmes processus et tables de routage par routeur virtuel. À l'aide de routeurs virtuels, vous créez des réseaux séparés logiquement sur le même réseau physique pour assurer la confidentialité du trafic qui traverse chaque routeur virtuel.

Comme les tables de routage sont distinctes, vous pouvez utiliser les mêmes espaces adresse ou se chevaucher dans les routeurs virtuels. Par exemple, vous pourriez utiliser l'espace d'adresse 192.168.1.0/24 pour deux routeurs virtuels distincts, pris en charge par deux interfaces physiques distinctes.

Notez qu'il existe des tableaux de gestion et de routage des données distincts par routeur virtuel. Par exemple, si vous affectez une interface de gestion uniquement à un routeur virtuel, la table de routage pour cette interface est distincte des interfaces de données affectées au routeur virtuel.

Configuration des politiques pour qu'elles soient compatibles avec les routeurs virtuels

Lorsque vous créez un routeur virtuel, la table de routage de ce routeur virtuel est automatiquement séparée du routeur virtuel global ou de tout autre routeur virtuel. Cependant, les politiques de sécurité ne prennent pas automatiquement en charge les routeurs virtuels.

Par exemple, si vous écrivez une règle de contrôle d'accès qui s'applique à « toute » zone de sécurité de source ou de destination, la règle s'appliquera à toutes les interfaces de tous les routeurs virtuels. Cela pourrait en fait être exactement ce que vous voulez. Par exemple, tous vos clients peuvent vouloir bloquer l'accès à une même liste de catégories d'URL répréhensibles.

Toutefois, si vous devez appliquer une politique à l'un des routeurs virtuels mais pas à d'autres, vous devez créer des zones de sécurité qui contiennent les interfaces de ce seul routeur virtuel uniquement. Ensuite, utilisez les zones de sécurité contraintes de virtual-routeur-constrained dans les critères de source et de destination de la politique de sécurité.

En utilisant des zones de sécurité dont les appartenances sont limitées aux interfaces affectées à un seul routeur virtuel, vous pouvez écrire des règles compatibles avec les routeurs virtuels dans les politiques suivantes :

- Politique de contrôle d'accès.
- Politiques de prévention des intrusions et de fichiers.
- Politiques de déchiffrement SSL.
- Politique d'identité et mappages utilisateur-adresse IP. Si vous utilisez des espaces d'adresses qui se chevauchent dans les routeurs virtuels, assurez-vous de créer des domaines distincts pour chaque routeur virtuel et de les appliquer correctement dans les règles de politique d'identité.

Si vous utilisez des espaces adresses qui se chevauchent dans vos routeurs virtuels, vous devez utiliser des zones de sécurité pour vous assurer que les bonnes politiques sont appliquées. Par exemple, si vous utilisez l'espace d'adresse 192.168.1.0/24 dans deux routeurs virtuels distincts, une règle de contrôle d'accès qui spécifie simplement le réseau 192.168.1.0/24 s'appliquera au trafic dans les deux routeurs virtuels. Si ce n'est pas le résultat souhaité, vous pouvez limiter l'application de la règle en spécifiant également les zones de sécurité de source et de destination pour un seul des routeurs virtuels.

Pour les politiques qui n'utilisent pas de zones de sécurité, comme la NAT, vous pouvez écrire des règles spécifiques à un routeur virtuel en sélectionnant les interfaces affectées à un seul routeur virtuel comme interfaces de source et de destination. Si vous sélectionnez des interfaces de source et de destination de deux routeurs virtuels distincts, vous devez vous assurer que les routes sont appropriées entre les routeurs virtuels pour que la règle s'applique.

Routage entre routeurs virtuels

Vous pouvez configurer des routes statiques pour acheminer le trafic entre les routeurs virtuels.

Par exemple, si vous avez l'interface externe dans le routeur virtuel global, vous pouvez configurer des routes statiques par défaut dans chacun des autres routeurs virtuels pour envoyer le trafic vers l'interface externe.

Ensuite, tout trafic qui ne peut pas être acheminé dans un routeur virtuel donné est envoyé au routeur global pour le routage ultérieur.

Les routes statiques entre les routeurs virtuels sont appelées fuites de route, car vous faites fuiter du trafic vers un autre routeur virtuel. Lorsque vous communiquez des fuites de routes, par exemple des routages VR1 vers VR2, vous pouvez initier des connexions de VR2 à VR1 uniquement. Pour que le trafic passe de VR1 à VR2, vous devez configurer la route inverse. Lorsque vous créez une voie de routage statique vers une interface dans un autre routeur virtuel, vous n'avez pas besoin de préciser d'adresse de la passerelle. Sélectionnez simplement l'interface de destination.

Pour les routes inter-routeurs virtuels, le système recherche l'interface de destination dans le routeur virtuel source. Ensuite, il recherche l'adresse MAC du prochain saut dans le routeur virtuel de destination. Ainsi, le routeur virtuel de destination doit avoir une route dynamique (acquise) ou statique pour l'interface sélectionnée pour l'adresse de destination.

La configuration de règles NAT qui utilisent des interfaces source et de destination dans différents routeurs virtuels peut également permettre au trafic d'être acheminé entre les routeurs virtuels. Si vous ne sélectionnez pas l'option permettant à la NAT d'effectuer une recherche de routage, la règle enverra simplement le trafic hors de l'interface de destination avec une adresse NAT chaque fois que la traduction de destination se produit. Cependant, le routeur virtuel de destination doit avoir une voie de routage pour l'adresse IP de destination traduite afin que la recherche du saut suivant puisse réussir.

Nombre maximal de routeurs virtuels par modèle de périphérique

Le nombre maximal de routeurs virtuels que vous pouvez créer dépend du modèle de périphérique. Le tableau suivant présente les limites maximales. Vous pouvez vérifier votre système en saisissant la commande **show vrf counters**, qui affiche le nombre maximal de routeurs virtuels définis par l'utilisateur pour cette plateforme, sans compter le routeur virtuel global. Les chiffres dans le tableau ci-dessous comprennent les routeurs utilisateur et globaux. Pour Firepower 4100/9300, ces chiffres s'appliquent au mode natif.

Pour les plateformes qui prennent en charge la capacité d'instances multiples, comme les Firepower 4100/9300, déterminez le nombre maximal de routeurs virtuels par instance de conteneur en divisant le nombre maximal de routeurs virtuels par le nombre de cœurs sur le périphérique, puis en multipliant par le nombre de cœurs affectés à de l'instance, en arrondissant au nombre entier inférieur le plus proche. Par exemple, si la plateforme prend en charge un maximum de 100 routeurs virtuels et qu'elle compte 70 cœurs, chaque cœur prendra en charge un maximum de 1,43 routeur virtuel (arrondi). Ainsi, une instance affectée de 6 cœurs prendrait en charge 8,58 routeurs virtuels, arrondis à 8, et une instance affectée de 10 cœurs prendrait en charge 14,3 routeurs virtuels (arrondis à la valeur inférieure, 14).

Modèle du périphérique	Routeurs virtuels maximums
ASA 5508-X ASA 5516-X	10
Firepower 1010	Les routeurs virtuels ne sont pas pris en charge sur ce modèle.
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower 2110	10

Modèle du périphérique	Routeurs virtuels maximums
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Firepower 4110	60
Firepower 4112	60
Firepower 4115	80
Firepower 4120	80
Firepower 4125	100
Firepower 4140	100
Firepower 4145	100
Firepower 4150	100
Appareils Cisco Firepower de série 9300, tous les modèles	100
Firewall Threat Defense Virtual, toutes les plateformes	30
ISA 3000	10

Lignes directrices pour les routeurs virtuels

Directives relatives aux modèles de périphériques

Vous pouvez configurer des routeurs virtuels sur tous les modèles de périphériques pris en charge, à l'exception des suivants :

- Firepower 1010

Directives supplémentaires

- Vous ne pouvez configurer le protocole EIGRP que sur le routeur virtuel global.
  - RIP
  - EIGRP
  - IS-IS
  - BGPv6
  - Routage multidiffusion

  - Routage basé sur une stratégie
  - VPN
- Vous pouvez configurer les fonctionnalités suivantes séparément pour chaque routeur virtuel :
  - Routes statiques et leurs moniteurs SLA.
  - OSPFv2
  - BGPv4
- Les fonctionnalités suivantes sont utilisées par le système lors des requêtes ou des communications avec le système distant (trafic initial). Ces fonctionnalités utilisent uniquement les interfaces du routeur virtuel global. Si vous configurez une interface pour cette fonctionnalité, elle doit appartenir au routeur virtuel global. En règle générale, lorsque le système doit rechercher une route pour atteindre un serveur externe à des fins de gestion, il effectue la recherche dans le routeur virtuel global.
  - Serveur DNS, lorsqu'il est utilisé pour résoudre les noms complets utilisés dans les règles de contrôle d'accès ou pour résoudre des noms pour la commande**ping**. Si vous spécifiez **any (tout)** comme interface pour un serveur DNS, le système prend en compte les interfaces uniquement du routeur virtuel global.
  - Serveur AAA ou domaine d'identité lorsqu'il est utilisé avec un VPN. Vous pouvez configurer le VPN uniquement sur des interfaces dans le routeur virtuel global, donc les serveurs AAA externes utilisés pour le VPN, comme Active Directory, doivent être accessibles par l'intermédiaire d'une interface dans le routeur virtuel global.
  - Serveur Syslog.
  - SNMP.
- Dans la NAT, si vous spécifiez des interfaces source et destination associées à des routeurs virtuels différents, la règle NAT détourne le trafic d'un routeur virtuel vers un autre. Assurez-vous de ne pas combiner les interfaces dans les règles de NAT par erreur. Normalement, les interfaces source et destination sont utilisées et la table de routage est ignorée, y compris pour les traductions de destination dans la NAT Toutefois, si la règle NAT doit effectuer une recherche de routage, celle-ci se fait uniquement dans la table VRF de l'interface entrante. Au besoin, définissez les routes statiques dans le routeur virtuel source pour l'interface de destination. Si vous laissez l'interface à **any**, la règle s'applique à toutes les interfaces, quel que soit leur appartenance au routeur virtuel. Lorsque vous utilisez des routeurs virtuels, testez soigneusement vos règles de NAT pour vous assurer d'obtenir le comportement attendu. Si vous omettez de définir une fuite de route nécessaire, il peut arriver que la règle ne corresponde pas à tout le trafic attendu et que la traduction ne soit pas appliquée.
- Si vous configurez des routes entre routeurs virtuels, par exemple en divulguant une route d'un routeur virtuel vers un second, le système effectue la recherche de l'interface de destination dans le routeur virtuel source. Ensuite, il recherche l'adresse MAC du prochain saut dans le routeur virtuel de destination. Ainsi, le routeur virtuel de destination doit avoir une route dynamique (acquise) ou statique pour l'interface sélectionnée pour l'adresse de destination.
- Lorsque vous utilisez des routes entre routeurs virtuels (routes divulguées), par exemple du routeur virtuel 1 vers le routeur virtuel 2, vous n'avez pas à configurer une route miroir (inversée) dans le routeur virtuel 2 pour permettre le trafic de retour. Toutefois, si vous souhaitez autoriser des connexions dans les deux sens, veillez à divulguer la route dans les deux directions, du routeur virtuel 1 au routeur virtuel 2 et du routeur virtuel 2 au routeur virtuel 1.

- Si vous déplacez une interface d'un routeur virtuel à un autre, toutes les fonctionnalités configurées pour l'interface sont conservées. Examinez la configuration pour vous assurer que les routes statiques, les adresses IP et les autres politiques ont du sens dans le contexte du nouveau routeur virtuel.
- Si vous utilisez des espaces d'adresses qui se chevauchent dans plusieurs routeurs virtuels, sachez que les mappages statiques de balises de groupe de sécurité (SGT) vers des adresses IP téléchargés à partir du Cisco Identity Services Engine (ISE) ne reconnaissent pas les routeurs virtuels. Configurez des domaines d'identité distincts pour chaque routeur virtuel si vous devez créer différents mappages SGT par routeur virtuel. Cela n'est pas nécessaire si vous souhaitez mettre en correspondance les mêmes adresses IP avec le même numéro SGT dans chaque routeur virtuel.
- Si vous utilisez des espaces d'adresses qui se chevauchent dans plusieurs routeurs virtuels, les données du tableau de bord peuvent induire en erreur. Les connexions pour la même adresse IP sont agrégées, de sorte qu'il apparaîtra qu'il y a eu plus de trafic vers ou depuis une adresse donnée lorsqu'elle est partagée par deux points terminaux ou plus. Si vous créez soigneusement vos politiques d'identité à l'aide de domaines d'identité distincts, les statistiques basées sur l'utilisateur devraient être plus exactes.
- Vous ne pouvez pas utiliser des ensembles d'adresses DHCP qui se chevauchent dans des routeurs virtuels distincts.
- Vous pouvez utiliser la configuration automatique du serveur DHCP uniquement sur une interface du routeur virtuel global. La configuration automatique n'est pas prise en charge pour les interfaces affectées à un routeur virtuel défini par l'utilisateur.
- Si vous déplacez une interface d'un routeur virtuel à un autre, y compris du routeur virtuel global vers un nouveau routeur, toutes les connexions existantes par l'intermédiaire de l'interface sont abandonnées.
- La politique de renseignements sur la sécurité n'est pas compatible avec les routeurs virtuels. Si vous ajoutez une adresse IP, une URL ou un nom DNS à la liste de blocage, tous les routeurs virtuels le bloqueront.

Gestion des routeurs virtuels

Vous pouvez créer plusieurs instances de routage et de transfert virtuels (VRF), appelées routeurs virtuels, pour maintenir des tables de routage distinctes pour des groupes d'interfaces. Étant donné que chaque routeur virtuel possède sa propre table de routage, vous pouvez assurer une séparation nette du trafic circulant à travers le périphérique.

Vous pouvez ainsi fournir une assistance à deux clients distincts ou plus concernant un ensemble d'équipements réseau communs. Vous pouvez également utiliser des routeurs virtuels pour renforcer la séparation entre les éléments de votre propre réseau, par exemple en isolant un réseau de développement de votre réseau d'entreprise général.

Par défaut, le routage virtuel est désactivé. L'appareil entier utilise un seul ensemble de tables de routage globales, pour le trafic de données (par le biais) et de gestion (vers/à partir du boîtier).

Lorsque vous activez le routage virtuel, la page de routage initiale est une liste des routeurs virtuels définis sur le système. Si vous n'activez pas les routeurs virtuels, la page de routage initiale est une liste des routes statiques définies sur le système.

Il y a toujours un routeur virtuel global. Le routeur global contient toutes les interfaces que vous n'avez pas affectées aux routeurs virtuels individuels.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous n'avez pas encore activé les routeurs virtuels, cliquez sur le lien **Add Multiple Virtual Routers** (Ajouter plusieurs routeurs virtuels), puis sur **Create First Custom Virtual Router** (Créer le premier routeur virtuel personnalisé).

La création du premier routeur virtuel est essentiellement la même que la création de routeurs virtuels supplémentaires. Pour en savoir plus, consultez Créer un routeur virtuel ou modifier les affectations d'interface, à la page 340.

Étape 3 Effectuez l'une des actions suivantes :

- Pour configurer les paramètres globaux de BGP, qui s'appliquent à tous les routeurs virtuels, cliquez sur le bouton **BGP Global Settings** (Paramètres globaux BGP). Vous configurez ces paramètres à l'aide de l'interface de ligne de commande Smart, qui est expliquée dans Configuration des objets Smart CLI, à la page 880. Configurez les paramètres globaux de BGP uniquement si vous configurez BGP dans un ou plusieurs routeurs virtuels.
- Pour créer un nouveau routeur virtuel, cliquez sur le bouton + au-dessus du tableau.
- Pour modifier les propriétés de routage d'un routeur virtuel, par exemple, pour créer des routes statiques ou définir des processus de routage, cliquez sur l'icône d'affichage ( ) dans la case Action du routeur virtuel.
- Pour modifier le nom, la description ou les affectations d'interface pour un routeur virtuel, cliquez sur l'icône d'affichage ( ) dans la case Action pour le routeur virtuel, puis sélectionnez l'onglet **Virtual Router Properties** (Propriétés du routeur virtuel).
- Pour basculer entre les routeurs virtuels lorsque vous les affichez, cliquez sur la flèche vers le bas à côté du nom du routeur virtuel (au-dessus de la table de routage) et sélectionnez le routeur virtuel souhaité. Vous pouvez revenir à la page de liste en cliquant sur la flèche **Go Back to Virtual Routers** (Revenir aux routeurs virtuels) ( ).
- Pour supprimer un routeur virtuel, cliquez sur l'icône de suppression ( ) dans la case Action du routeur virtuel ou sur l'icône de suppression à côté du nom du routeur virtuel lorsque vous affichez le contenu du routeur virtuel. Lorsque vous supprimez le dernier routeur virtuel (autre que le routeur global, que vous ne pouvez pas supprimer), le VRF est désactivé.
- Pour surveiller le routage dans un routeur virtuel, cliquez sur le lien de l'une des commandes **show** dans le tableau de ce routeur virtuel. Cliquez sur la commande pour ouvrir la console CLI, où vous pouvez examiner le résultat de la commande CLI. Vous pouvez afficher les informations sur les routes, OSPF et les voisins OSPF. Notez que le résultat de la commande est basé sur la configuration déployée ; vous ne verrez rien concernant les modifications non déployées.

  Vous pouvez également exécuter ces commandes en les sélectionnant dans la liste déroulante **Commands** (Commandes) lorsque vous affichez le routeur virtuel.

Créer un routeur virtuel ou modifier les affectations d'interface

Avant de pouvoir configurer des routes statiques ou un processus de routage sur un routeur virtuel, vous devez créer le routeur et lui affecter des interfaces.

Avant de commencer

Accédez à la page **Interfaces** et assurez-vous que chaque interface que vous souhaitez ajouter au routeur virtuel a un nom. Vous ne pouvez pas ajouter d'interface à un routeur virtuel tant qu'il n'a pas de nom.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)** > **Routing (Routage)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Si vous n'avez pas encore créé de routeur virtuel, cliquez sur le lien **Add Multiple Virtual Router**s (Ajouter plusieurs routeurs virtuels), puis sur **Create First Custom Virtual Router** (Créer le premier routeur virtuel personnalisé).
- Cliquez sur le bouton **+** au-dessus de la liste des routeurs virtuels pour en créer un nouveau.
- Cliquez sur l'icône de modification ( ) d'un routeur virtuel afin de modifier ses propriétés et la liste d'interfaces.
- Lorsque vous affichez un routeur virtuel, cliquez sur l'onglet **Virtual Router Properties** (Propriétés du routeur virtuel) pour modifier les propriétés du routeur virtuel affiché.
- Lorsque vous affichez un routeur virtuel, cliquez sur la flèche vers le bas à côté du nom du routeur virtuel, puis cliquez sur**Create New Virtual Router** (Créer un nouveau routeur virtuel).

Étape 3 Configurez les propriétés du routeur virtuel :

- **Name** (Nom) : nom du routeur virtuel.
- **Description** : une description facultative du routeur virtuel.
- **Interfaces** : cliquez sur le signe plus **(+)** pour sélectionner chaque interface qui doit faire partie du routeur virtuel. Pour supprimer une interface, passez le curseur sur l'interface et cliquez sur **X** sur le côté droit de la carte d'interface. Vous pouvez affecter des interfaces physiques, des sous-interfaces, des groupes de ponts et des EtherChannels à un routeur virtuel, mais pas des VLAN.

  La table de routage sera limitée à ces interfaces, sauf si vous communiquez intentionnellement les routes vers d'autres interfaces dans la table de routage virtuelle.

  Vous pouvez attribuer l'interface de diagnostic (Management X/Y) uniquement au routeur virtuel global.

Étape 4 Cliquez sur **OK** ou sur **Save** (Enregistrer).

Vous êtes redirigé vers l'affichage de ce routeur virtuel, où vous pouvez configurer des routes statiques ou des processus de routage.

Configurer Static Routes (routes statiques) et Routing Processes (processus de routage) dans un routeur virtuel

Chaque routeur virtuel possède ses propres routes statiques et processus de routage, qui fonctionnent séparément de ceux définis pour tout autre routeur virtuel.

Lorsque vous configurez des routes statiques, vous pouvez sélectionner des interfaces de destination qui se trouvent à l'extérieur du routeur virtuel. Cela entraîne une fuite de la route dans le routeur virtuel qui contient l'interface de destination. Assurez-vous de ne faire fuiter que les routes nécessaires, afin de ne pas envoyer plus de trafic que vous ne le souhaitez vers l'autre routeur virtuel. Par exemple, si vous disposez d'un seul chemin d'accès à Internet, il est logique de faire fuiter les routes de chaque routeur virtuel vers le routeur virtuel orienté vers Internet pour le trafic destiné à Internet.

Procédure

Étape 1 Choisissez **Device (Appareil)** > **Routing (Routage)**.

Étape 2 Cliquez sur l'icône d'affichage ( ) dans la case Action pour que le routeur virtuel l'ouvre.

Étape 3 Effectuez l'une des actions suivantes :

- Pour configurer des routes statiques, cliquez sur l'onglet **Static Routing** (routage statique), puis créez ou modifiez les routes. Pour de plus amples renseignements, voir Configuration des routes statiques, à la page 325.
- Pour configurer des zones de trafic à coût unique (Equal-Cost Multi-Path, ECMP), cliquez sur l'onglet **ECMP Traffic Zones** (zones de trafic ECMP), puis créez les zones. Pour de plus amples renseignements, voir Configuration des zones de trafic ECMP, à la page 328.
- Pour configurer le processus de routage BGP, cliquez sur l'onglet **BGP**, puis créez l'objet Smart CLI nécessaire pour définir le processus. Pour de plus amples renseignements, voir Protocole de routage BGP, à la page 419.

  Il existe également des paramètres globaux pour BGP qui s'appliquent à tous les routeurs virtuels. Vous devez revenir à la page de liste des routeurs virtuels pour cliquer sur le bouton **BGP Global Settings** (paramètres globaux BGP) pour configurer ces propriétés.
- Pour configurer le processus de routage OSPF, cliquez sur l'onglet **OSPF**, puis créez les objets Smart CLI nécessaires pour définir jusqu'à 2 processus et les configurations d'interface associées. Pour de plus amples renseignements, voir Open Shortest Path First (OSPF), à la page 379.
- (Routeur virtuel global uniquement.) Pour configurer le processus de routage EIGRP, cliquez sur l'onglet **EIGRP**, puis créez l'objet Smart CLI nécessaire pour définir un seul processus. Pour de plus amples renseignements, voir Protocole de routage de passerelle intérieure amélioré (EIGRP), à la page 401.

Supprimer un routeur virtuel

Si vous n'avez plus besoin d'un routeur virtuel, vous pouvez le supprimer. Vous ne pouvez pas supprimer le routeur virtuel global.

Lorsque vous supprimez un routeur virtuel, vous supprimez également toutes les routes statiques et les processus de routage configurés dans le routeur virtuel.

Toutes les interfaces affectées au routeur virtuel sont réaffectées au routeur global.

Procédure

Étape 1 Choisissez **Device (Périphérique)** > **Routing (Routage)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Dans la liste des routeurs virtuels, cliquez sur l'icône de suppression ( ) dans la colonne Action pour le routeur virtuel.
- Lorsque vous affichez le routeur virtuel que vous souhaitez supprimer, cliquez sur l'icône de suppression ( ) à côté du nom du routeur.

Vous êtes invité à confirmer que vous souhaitez supprimer le routeur virtuel.

Étape 3 Cliquez sur **OK** pour confirmer la suppression.

Exemples pour les routeurs virtuels

Les rubriques suivantes fournissent des exemples d'implémentation de routeurs virtuels.

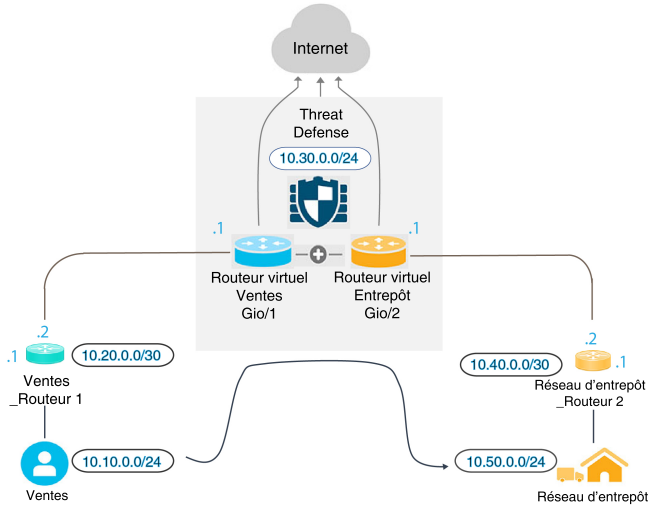
Sujets connexes

Sécuriser le trafic de réseaux dans plusieurs routeurs virtuels sur un VPN de site à site, à la page 698
Comment autoriser l'accès au VPN d'accès à distance aux réseaux internes dans différents routeurs virtuels., à la page 775

Comment effectuer un routage vers un serveur distant à l'aide de routeurs virtuels

Lorsque vous utilisez des routeurs virtuels, vous pouvez avoir une situation où les utilisateurs d'un routeur virtuel ont besoin d'accéder à un serveur qui n'est accessible que par l'intermédiaire d'un routeur virtuel distinct.

Reportez-vous à l'illustration suivante. Les ordinateurs de travail de l'équipe des ventes sont connectés au routeur virtuel des ventes. Les serveurs d'entrepôt sont connectés par l'intermédiaire du routeur virtuel de l'entrepôt. Si l'équipe de vente doit rechercher des informations sur le serveur de l'entrepôt dont l'adresse IP est 10.50.0.5/24, vous devez divulguer une route du routeur virtuel des ventes vers le routeur virtuel de l'entrepôt. Le routeur virtuel de l'entrepôt doit également avoir une voie de routage vers le serveur de l'entrepôt, qui se trouve de plusieurs sauts derrière le routeur de l'entrepôt 2.



Avant de commencer

Cet exemple suppose que vous avez déjà configuré :

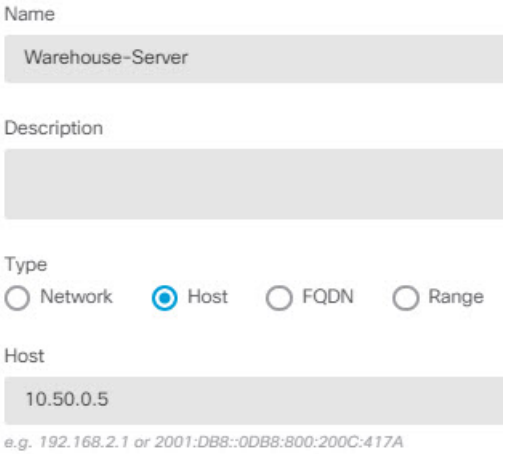
- Les routeurs virtuels Ventes et Entrepôt sur le périphérique Firewall Threat Defense, avec GigabitEthernet 0/1 attribué aux Ventes et GigabitEthernet 0/2 attribué à l'Entrepôt.
- Le routeur de ventes 1 a une route statique ou dynamique qui enverra le trafic vers 10.50.0.5/24 à partir de l'interface 10.20.0.1/30.

Procédure

Étape 1 Créez l'objet réseau pour 10.50.0.5/24 ou 10.50.0.0/24. Créez également l'objet pour la passerelle, 10.40.0.2/30.

Si vous souhaitez limiter le routage à l'adresse IP unique du serveur d'entrepôt, utilisez un objet hôte pour définir 10.50.0.5. Sinon, si l'équipe de vente doit avoir accès à d'autres systèmes dans l'entrepôt, créez un objet réseau pour le réseau 10.50.0.0/24. Dans cet exemple, nous créerons une route vers l'adresse IP de l'hôte.

a) Choisissez **Objects** (Objets), puis **Networks** (Réseaux) dans la table des matières.
b) Cliquez sur +, puis complétez les propriétés d'objet pour le serveur d'entrepôt :



c) Cliquez sur **OK**.

d) Cliquez sur **+**, puis complétez les propriétés d'objet pour la passerelle du routeur vers le réseau de l'entrepôt :



e) Cliquez sur **OK**.

Étape 2 Définissez la fuite de route dans Ventes qui pointe vers l'interface Gi0/2 dans le routeur virtuel de l'entrepôt.

Dans cet exemple, Gi0/1 est nommé inside, et Gi0/2 est nommé inside-2.

a) Sélectionnez **Device** (Périphérique), puis cliquez sur **View Configuration** (Afficher la configuration) dans le résumé **Routing** (Routage).

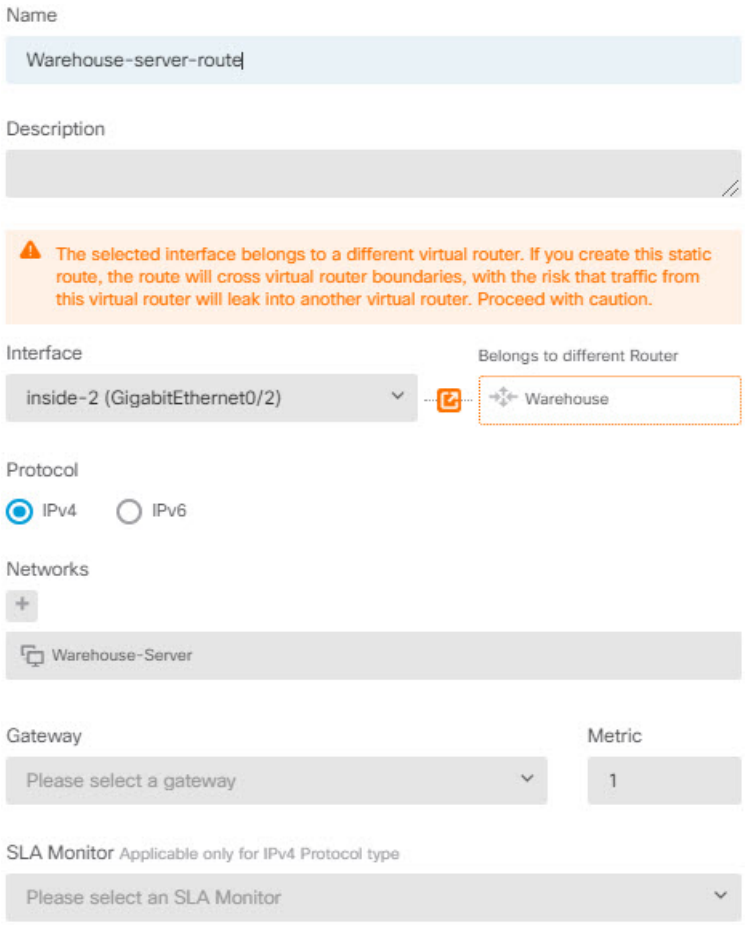
b) Dans la liste des routeurs virtuels, cliquez sur l'icône d'affichage ( ) dans la colonne d'action du routeur virtuel de ventes.

c) Dans l'onglet **Static Routing** (routage statique), cliquez sur le signe **plus (+)** et configurez le routage :

- **Name** (Nom) : tout nom convient, par exemple Entrepôt-serveur-route.
- **Interface** : sélectionnez **inside-2**. Vous verrez un avertissement indiquant que l'interface se trouve dans un autre routeur et que vous créez une fuite de route. C'est l'action souhaitée.
- **Protocole** : pour cet exemple, utilisez **IPv4**. Vous pouvez également utiliser des adresses IPv6 pour mettre en œuvre cet exemple.

- **Networks** (Réseaux) : sélectionnez l'objet Warehouse-Server.
- **Gateway** (passerelle) : laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :

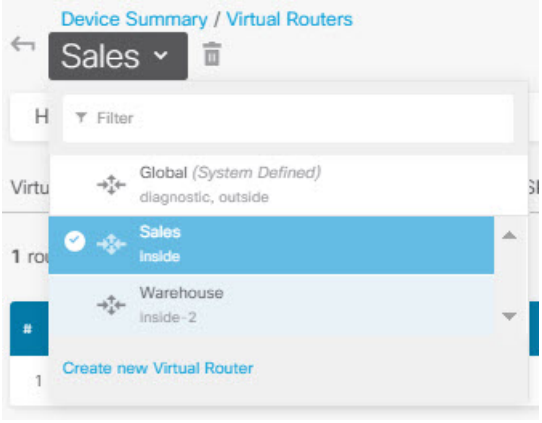


d) Cliquez sur **OK**.

Étape 3 Dans le routeur virtuel de l'entrepôt, définissez la route qui pointe vers la passerelle du routeur de l'entrepôt 2.

Sinon, cela peut être fait en configurant un protocole de routage qui découvrirait dynamiquement la route à partir du routeur de l'entrepôt 2. Pour cet exemple, nous définirons la route statique.

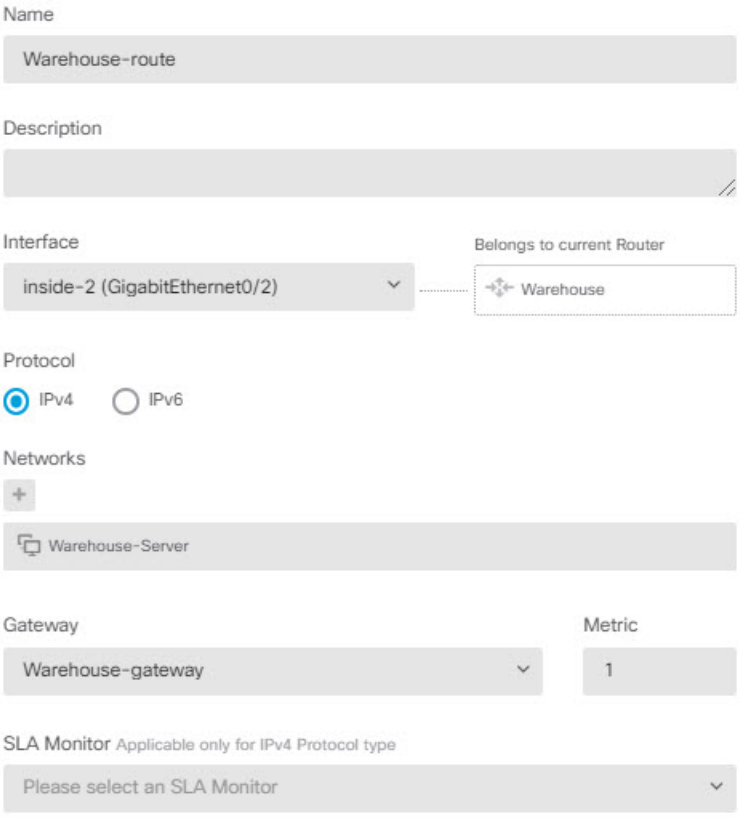
a) Dans la liste déroulante du routeur virtuel qui indique actuellement Ventes, sélectionnez le routeur virtuel de l'entrepôt pour changer de routeur.



b) Dans l'onglet **Static Routing** (routage statique), cliquez sur le signe **plus (+)** et configurez le routage :

- **Name** (Nom) : tout nom convient, par exemple Route de l'entrepôt.
- **Interface** : sélectionnez **inside-2**.
- **Protocole** : sélectionnez **IPv4**.
- **Networks** (Réseaux) : sélectionnez l'objet Warehouse-Server.
- **Gateway** (Passerelle) : Sélectionnez l'objet Warehouse-Gateway.

La boîte de dialogue doit ressembler à ce qui suit :

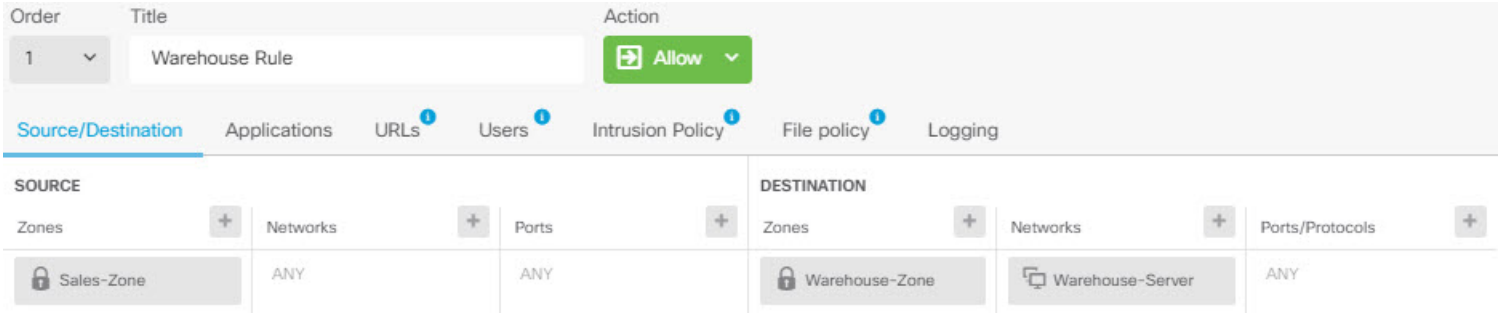


c) Cliquez sur **OK**.

Étape 4 Assurez-vous qu'il existe une règle de contrôle d'accès qui permet l'accès au serveur d'entrepôt.

La règle la plus simple permettrait le trafic des interfaces source du routeur virtuel des ventes vers les interfaces de destination du routeur virtuel d'entrepôt pour l'objet réseau de destination Warehouse-Server. Vous pouvez appliquer l'inspection de prévention des intrusions au trafic comme vous le souhaitez.

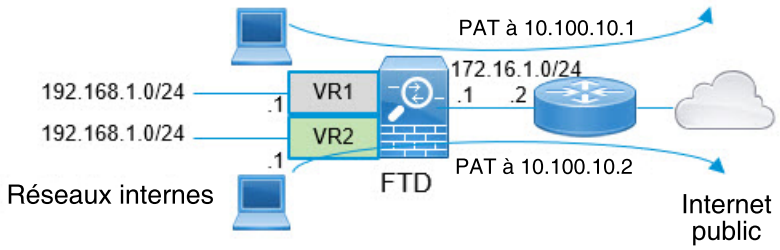
Par exemple, si les interfaces dans Sales se trouvent dans la zone de sécurité Sales-Zone et que celles de l'entrepôt sont dans la zone de sécurité Warehouse-Zone, la règle de contrôle d'accès ressemblera à ce qui suit :



Fournir un accès Internet à plusieurs routeurs virtuels avec des espaces d'adresses en chevauchement

Lorsque vous utilisez des routeurs virtuels, vous pouvez avoir la même adresse réseau pour les interfaces qui résident dans des routeurs distincts. Par exemple, les interfaces vr1-inside et vr2-inside sur FTD sont définies pour utiliser l'adresse IP 192.168.1.1/24 et gérer les points de terminaison sur leur segment dans le réseau 192.168.1.0/24. Cependant, comme les adresses IP acheminées dans ces routeurs virtuels distincts sont identiques, vous devez gérer avec soin le trafic qui quitte les routeurs virtuels pour vous assurer que le trafic de retour se dirige vers la bonne destination.

Pour autoriser l'accès Internet à partir de deux routeurs virtuels qui utilisent le même espace d'adresses, vous devez appliquer les règles NAT séparément aux interfaces de chaque routeur virtuel, idéalement en utilisant des pools NAT ou PAT distincts. Vous pouvez utiliser PAT pour traduire les adresses sources de virtual router 1 en 10.100.10.1 et, pour celles de virtual router 2, en 10.100.10.2. L'illustration suivante montre cette configuration, où l'interface externe accessible à Internet fait partie du routeur global. Vous devez définir les règles NAT/PAT avec l'interface source explicitement sélectionnée, car l'utilisation de « any » comme interface source empêche le système d'identifier correctement la source, étant donné que la même adresse IP peut exister sur deux interfaces différentes.



Remarque Cet exemple est simplifié : chaque routeur virtuel contient une seule interface. Si un routeur virtuel « interne » possède plusieurs interfaces, vous devez créer les règles NAT pour chaque interface « interne ». Même si certaines interfaces dans les routeurs virtuels n'utilisent pas des espaces d'adresses en chevauchement, sélectionner explicitement l'interface source dans les règles NAT peut faciliter le dépannage et assurer une séparation plus nette du trafic Internet sortant des routeurs virtuels.

Procédure

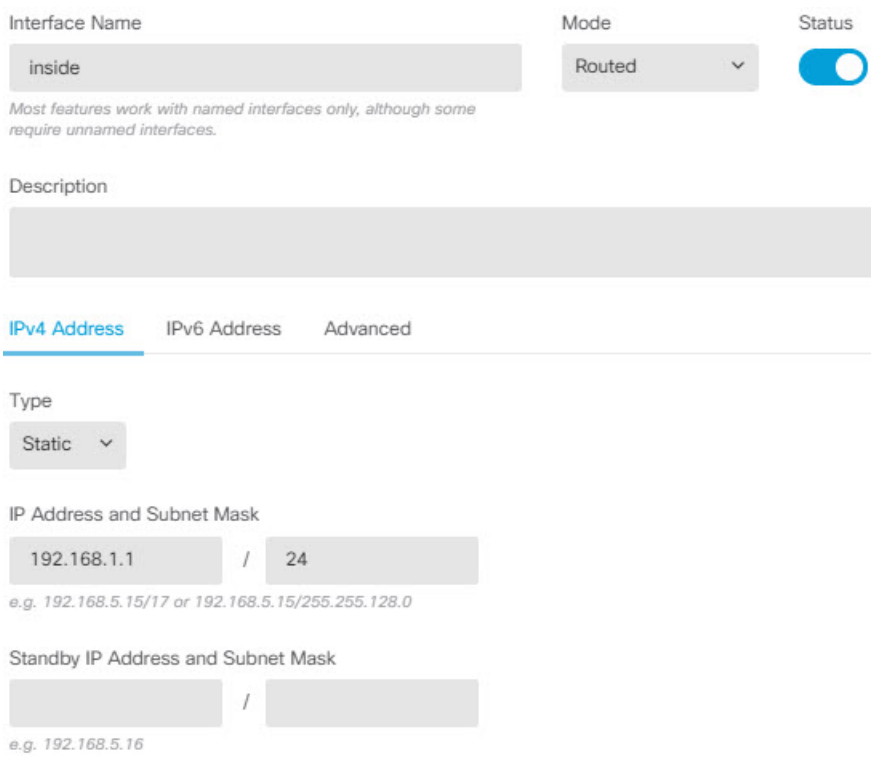
Étape 1 Configurez l'interface interne pour le routeur virtuel 1 (VR1).

a) Cliquez sur **Device** (appareil), puis sur **View All Interfaces** (afficher toutes les interfaces) dans le résumé **Interface**.

b) Cliquez sur l'icône de modification ( ) dans la colonne Action de l'interface que vous affecterez à VR1.

c) Configurez au moins les propriétés suivantes :

- **Name**(nom) : pour cet exemple, **inside**.
- **Mode** : Sélectionnez **Routed** (routage).
- **Status** (état) : activez l'interface.
- **Type** > **d'adresse IPv4** : sélectionnez **Static** (statique).
- **Adresse IPv4 et masque de sous-réseau** : saisissez 192.168.1.1/24.



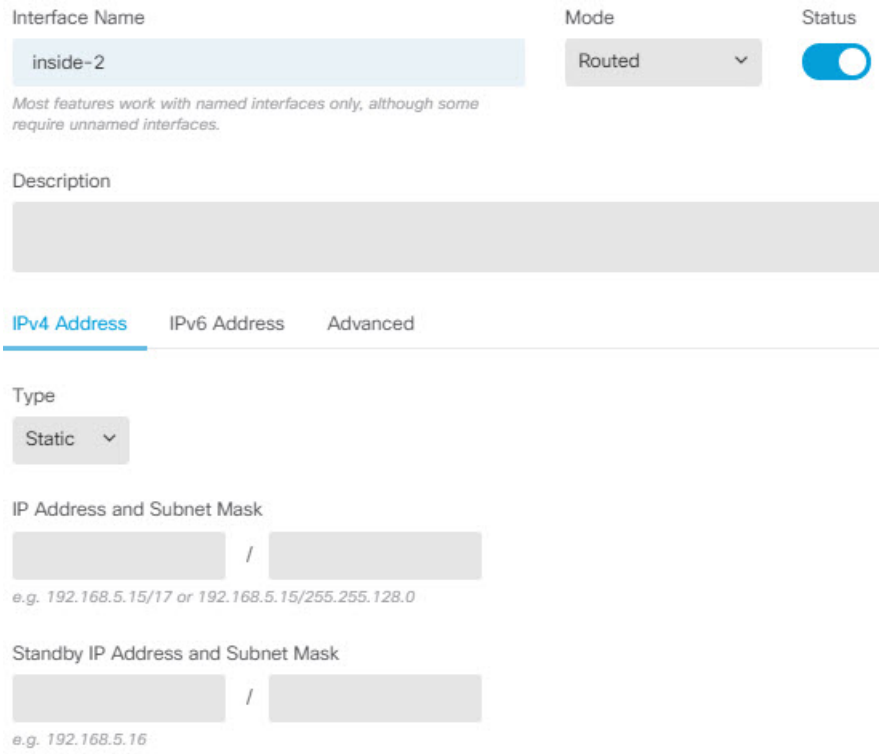
d) Cliquez sur **OK**.

Étape 2 Configurez l'interface interne-2 pour le routeur virtuel 2 (VR2), mais ne spécifiez pas l'adresse IP.

a) Sur la page de liste des interfaces, cliquez sur l'icône de modification ( ) dans la colonne Action de l'interface que vous affecterez à VR2.

b) Configurez au moins les propriétés suivantes :

- **Name** (nom) : pour cet exemple, **inside_2**.
- **Mode** : Sélectionnez **Routed** (routage).
- **Status** (état) : activez l'interface.
- **Type** > **d'adresse IPv4** : sélectionnez **Static** (statique).
- **Adresse IPv4 et masque de sous-réseau** : laissez ces champs vides. Si vous essayez de configurer la même adresse que l'interface interne à ce stade, le système affiche un message d'erreur et vous empêche de créer une configuration non fonctionnelle. Vous ne pouvez pas acheminer le trafic vers le même espace d'adresse en utilisant différentes interfaces sur le même routeur.



c) Cliquez sur **OK**.

Étape 3 Configurez le routeur virtuel VR1, y compris la fuite de route statique par défaut vers l'interface externe.

a) Choisissez **Device** (appareil), cliquez sur **View Configuration** (afficher la configuration) dans le résumé de **Routing** (routage).

b) Cliquez sur **Add Multiple Virtual Routers** (ajouter plusieurs routeurs virtuels) en haut de la page de routage.

c) Dans le coin inférieur droit du panneau explicatif, cliquez sur **Create First Custom Virtual Router** (créer le premier routeur virtuel personnalisé).

d) Remplissez les propriétés du routeur virtuel VR1.

- **Name** (nom) : saisissez VR1 ou un autre nom de votre choix.
- **Interfaces** : cliquez sur **+**, sélectionnez **inside**, puis cliquez sur **OK**.



e) Cliquez sur **OK**.

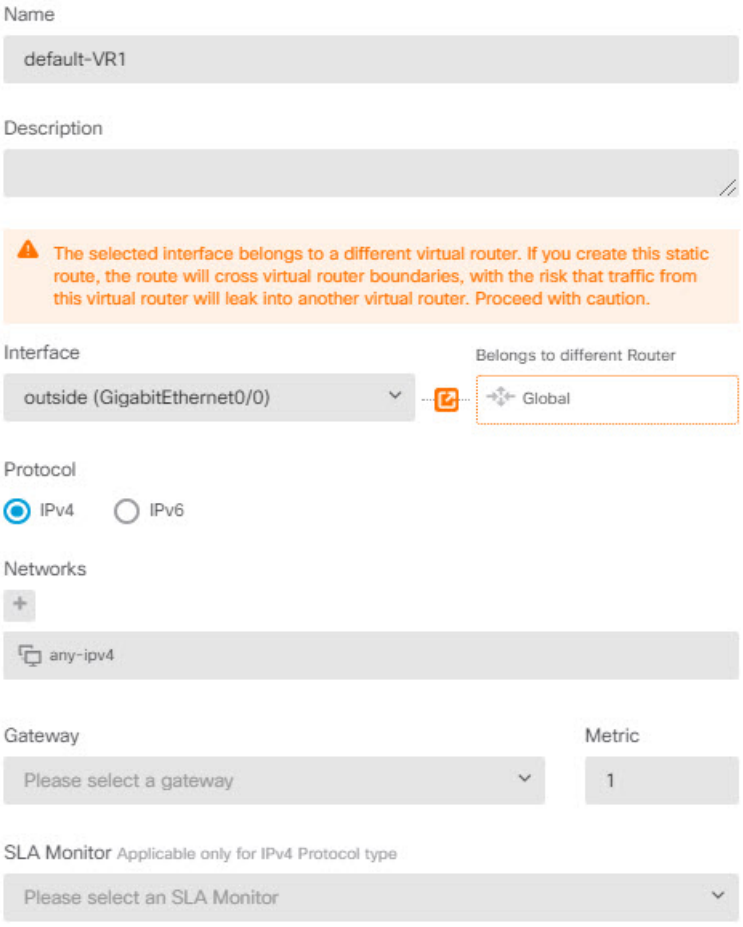
La boîte de dialogue se ferme et la liste des routeurs virtuels s'affiche.

f) Dans la liste des routeurs virtuels, cliquez sur l'icône d'affichage ( ) dans la colonne d'actions pour le routeur virtuel VR1.

g) Dans l'onglet **Static Routing** (routage statique), cliquez sur le signe **plus (+)** et configurez le routage :

- **Name** (nom) : n'importe quel nom suffit, tel que **default-VR1**.
- **Interface** : sélectionnez **outside**. Vous verrez un avertissement indiquant que l'interface se trouve dans un autre routeur et que vous créez une fuite de route. C'est l'action souhaitée.
- **Protocole** : pour cet exemple, utilisez **IPv4**.
- **Réseaux** : sélectionnez l'objet **any-ipv4**. Ce sera la voie de routage par défaut pour tout trafic qui ne peut pas être acheminé dans VR1.
- **Gateway** (passerelle) : laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



h) Cliquez sur **OK**.

Étape 4 Configurez le routeur virtuel VR2, y compris la fuite de route statique par défaut vers l'interface externe.

a) Lorsque vous affichez VR1, cliquez sur le bouton de retour (⇦) pour revenir à la liste des routeurs virtuels.
b) Cliquez sur + en haut de la liste.
c) Remplissez les propriétés du routeur virtuel VR2.

- **Name** (nom) : saisissez VR2 ou un autre nom de votre choix.
- **Interfaces** : cliquez sur +, sélectionnez **inside-2**, puis cliquez sur **OK**.



d) Cliquez sur **OK**.

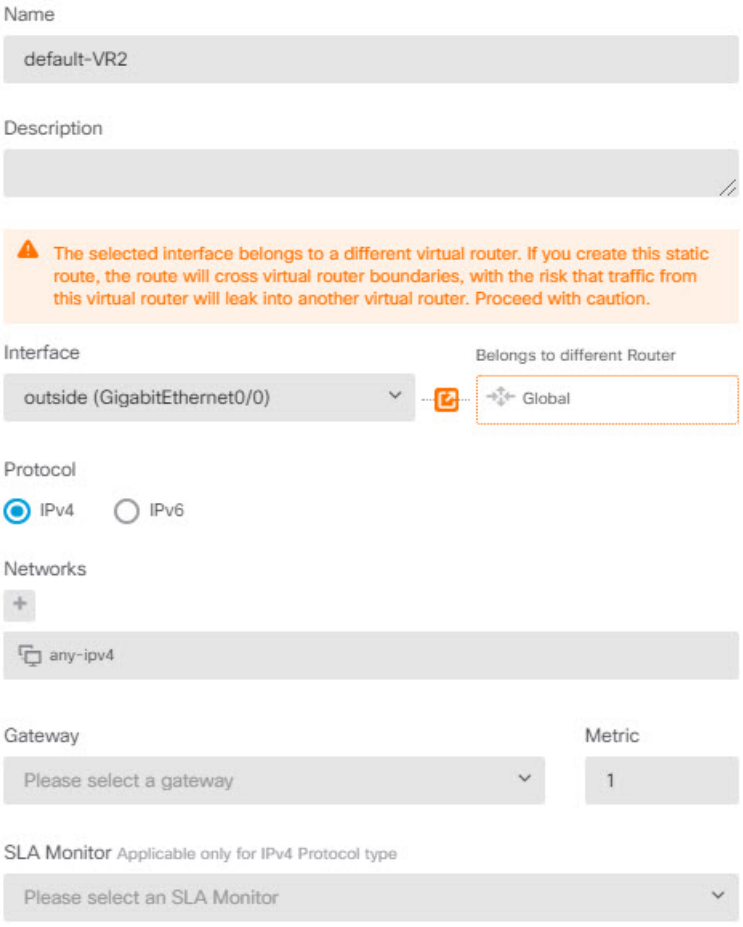
La boîte de dialogue se ferme et la liste des routeurs virtuels s'affiche.

e) Dans la liste des routeurs virtuels, cliquez sur l'icône d'affichage ( ) dans la colonne d'actions pour le routeur virtuel VR2.

f) Dans l'onglet **Static Routing** (routage statique), cliquez sur le signe **plus (+)** et configurez le routage :

- **Name** (nom) : n'importe quel nom suffit, tel que **default-VR2**.
- **Interface** : sélectionnez **outside**. Vous verrez un avertissement indiquant que l'interface se trouve dans un autre routeur et que vous créez une fuite de route. C'est l'action souhaitée.
- **Protocole** : pour cet exemple, utilisez **IPv4**.
- **Réseaux** : sélectionnez l'objet **any-ipv4**. Ce sera la voie de routage par défaut pour tout trafic qui ne peut pas être acheminé dans VR2.
- **Gateway** (passerelle) : laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



g) Cliquez sur **OK**.

Étape 5 Ajoutez la voie de routage par défaut dans le routeur global vers l'interface externe.

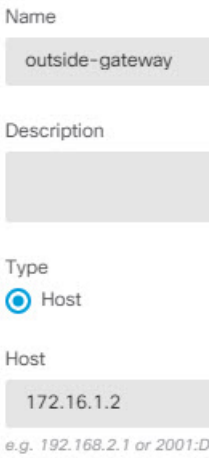
Le but de ce routage est d'affecter la passerelle correcte au trafic fuité des deux routeurs virtuels vers l'interface outside (externe) du routeur virtuel global.

a) Lorsque vous affichez VR2, cliquez sur le nom de VR2 en haut de la page pour ouvrir la liste des routeurs virtuels, puis sélectionnez le routeur Global.

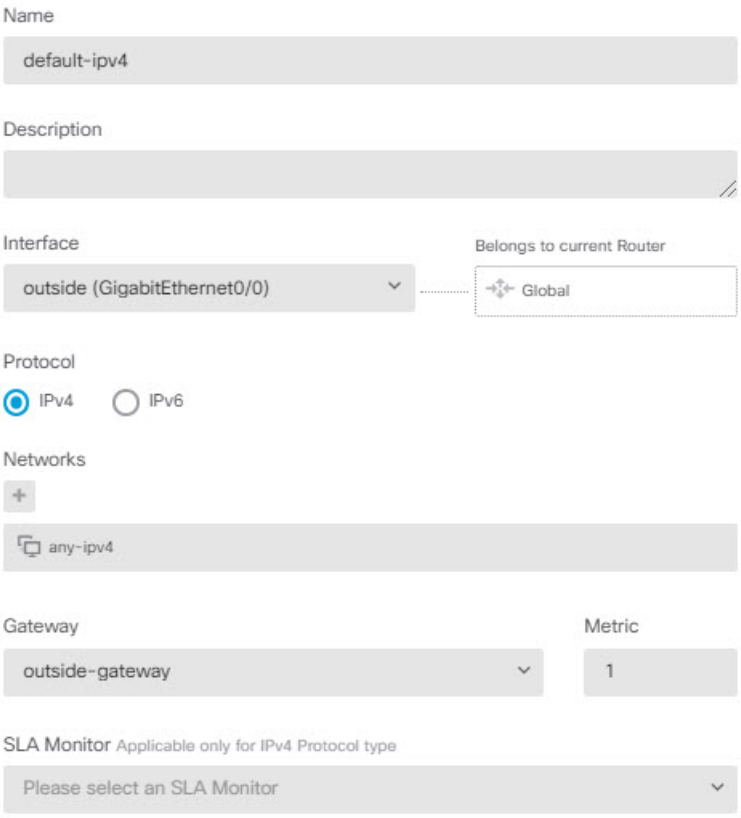


b) Dans l'onglet Static Routing (routage statique) du routeur Global, cliquez sur + et configurez le routage :

- **Name** (nom) : n'importe quel nom suffit, tel que par défaut-ipv4.
- **Interface** : sélectionnez **outside**.
- **Protocole** : pour cet exemple, utilisez **IPv4**.
- **Réseaux** : sélectionnez l'objet **any-ipv4**. Il s'agira de la voie de routage par défaut pour tout trafic IPv4.
- **Gateway** (passerelle) : si l'objet n'existe pas encore, cliquez sur **Create New Network Object** (Créer un nouvel objet réseau, puis définissez un objet hôte pour l'adresse IP de la passerelle à l'autre extrémité du lien réseau sur l'interface outside (externe), dans cet exemple 172.16.1.2. Après avoir créé l'objet, sélectionnez-le dans le champ Gateway (passerelle) du routage statique.



La boîte de dialogue doit ressembler à ce qui suit :



c) Cliquez sur **OK**.

Étape 6 Revenez à la page **Interfaces** et ajoutez l'adresse IP à inside-2.

a) Cliquez sur **Device** (appareil), puis sur **View All Interfaces** (afficher toutes les interfaces) dans le résumé **Interface**.

b) Cliquez sur l'icône de modification ( ) dans la colonne Action pour l'interface inside-2 que vous avez affectée à VR2.

c) Dans l'onglet **IPv4 Address** (adresse IPv4), saisissez 192.168.1.1/24 comme adresse IP et masque de sous-réseau.

d) Cliquez sur **OK**.

Vous n'obtenez pas d'erreur d'adresse IP en double cette fois, car les interfaces inside et inside-2 se trouvent désormais dans des routeurs virtuels distincts.

Étape 7 Créez la règle NAT pour appliquer la PAT de inside (interne) vers outside (externe) vers 10.100.10.1.

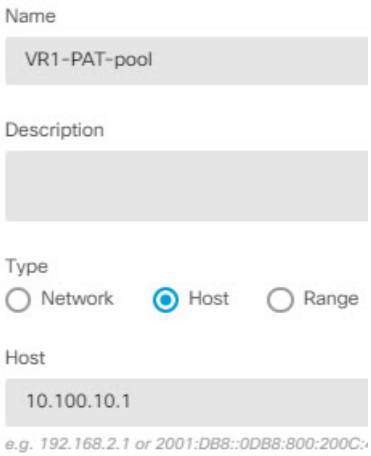
a) Choisissez **Policies** (politiques), puis cliquez sur **NAT**.

b) S'il existe déjà une règle NAT manuelle nommée InsideOutsideNatRule pour l'interface inside (interne) → outside (externe) appliquant la PAT d'interface, cliquez sur l'icône de modification ( ) pour la règle. Sinon, cliquez sur le signe **plus (+)** pour créer une nouvelle règle.

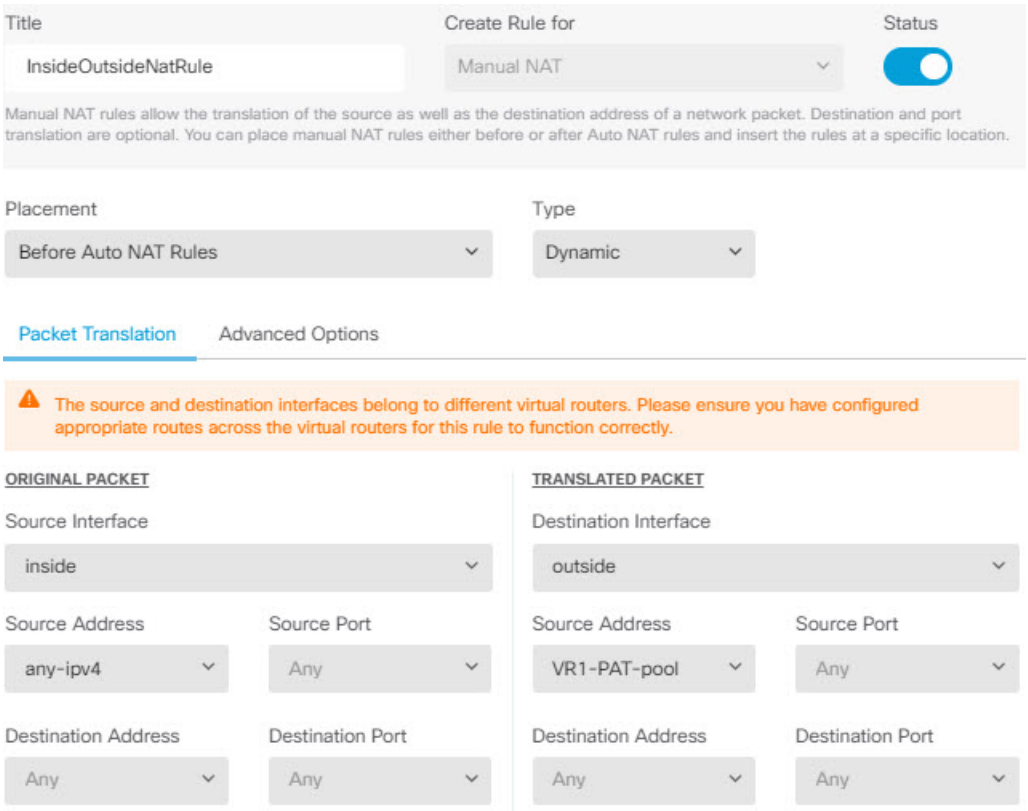
Si vous modifiez une règle existante, notez qu'un avertissement indique que les interfaces source et destination se trouvent dans des routeurs virtuels différents et que vous devez définir des routes. C'est ce que vous avez effectué plus tôt dans la procédure.

c) Si vous modifiez une règle existante, cliquez sur la flèche déroulante de **Translated Packet (Paquet traduit)** > **Source Address (Adresse source)**, puis cliquez sur **Create New Network** (Créer un nouveau réseau) (en supposant que vous n'avez pas encore d'objet hôte définissant 10.100.10.1).

d) Configurez l'objet réseau hôte pour l'adresse PAT. L'objet doit ressembler à ce qui suit :



e) Sélectionnez le nouvel objet comme **Translated Packet (Paquet traduit)** > **Source Address (Adresse source)**. La règle NAT doit ressembler à ce qui suit :



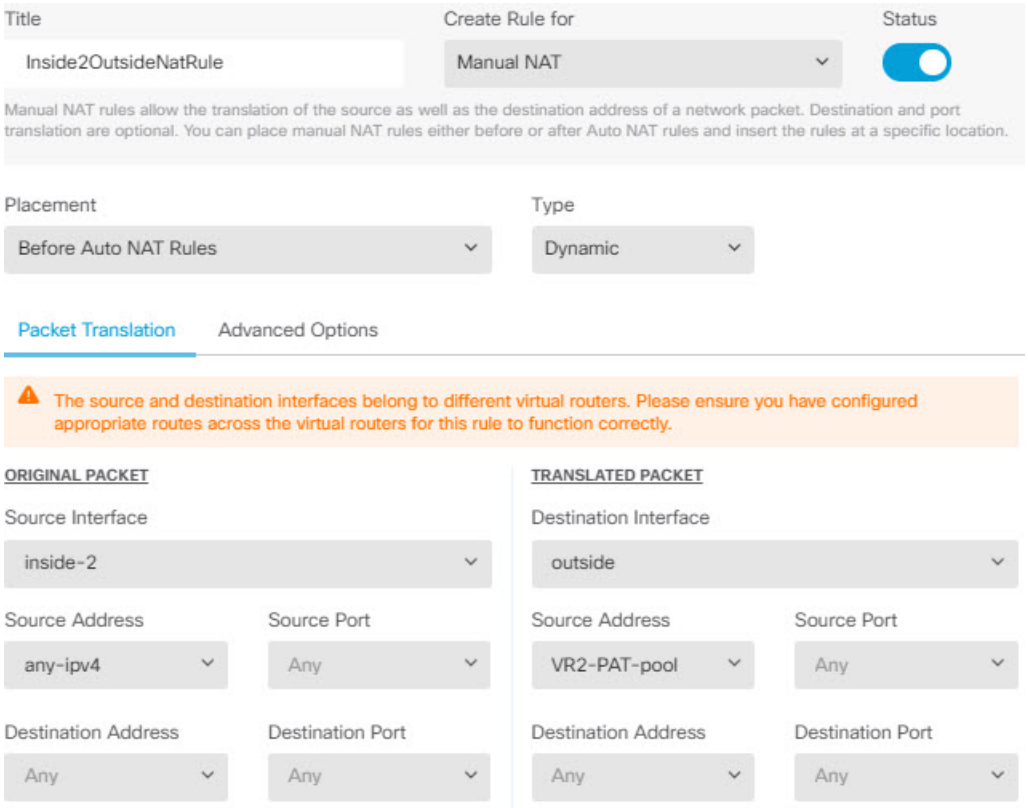
f) Cliquez sur **OK**.

Étape 8 Créez la règle NAT pour appliquer la PAT de inside-2 (interne-2) vers outside (externe) à 10.100.10.2.

Cette règle ressemblera exactement à celle de VR1, avec les exceptions suivantes :

- **Name (nom)** : il doit être unique, par exemple, Inside2OutsideNatRule.
- **Original Packet (Paquet d'origine)** > **Source Interface (Interface source)** : sélectionnez inside-2.
- **Translated Packet (Paquet traduit)** > **Source Address (Adresse source)** : créez un nouvel objet réseau d'hôte pour 10.100.10.2.

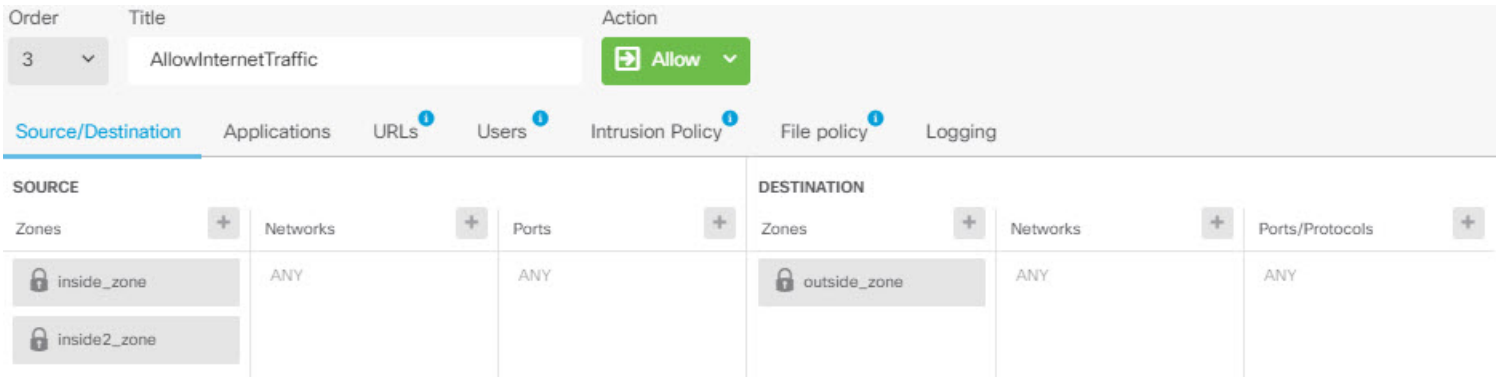
La règle devrait ressembler à ce qui suit :



Étape 9 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** et configurez une règle de contrôle d'accès pour autoriser le trafic de inside_zone et inside2_zone vers outside_zone.

Enfin, vous devez configurer la politique de contrôle d'accès pour permettre le trafic des interfaces inside et inside-2 vers l'interface outside (externe). Comme la règle de contrôle d'accès nécessite des zones de sécurité, vous devez créer des zones pour chacune de ces interfaces. Vous pouvez aussi créer une zone unique pour inclure inside et inside-2, mais il est probable que vous souhaiterez créer des règles supplémentaires, ici ou dans d'autres politiques, afin de différencier le traitement du trafic dans ces routeurs.

En supposant que vous créez des zones nommées d'après les interfaces, une règle de base qui permet à tout le trafic d'acheminer vers Internet ressemblera à ce qui suit. Vous pouvez appliquer une politique de prévention des intrusions à cette règle selon vos besoins. Vous pouvez définir des règles supplémentaires pour bloquer le trafic indésirable, par exemple pour appliquer un filtrage d'URL.



Surveillance des routeurs virtuels

Pour surveiller et dépanner les routeurs virtuels, ouvrez la console de l'interface de ligne de commande ou connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes. Vous pouvez également sélectionner certaines de ces commandes dans le menu **Commands** (Commandes) sur la page Routing (Routage).

- **show vrf** affiche les renseignements sur les routeurs virtuels définis sur le système.
- **show ospf** [**vrf** *name* | **all**]

  Affiche les informations sur le processus OSPF dans un routeur virtuel. Vous pouvez spécifier un routeur virtuel pour voir les informations sur le processus dans ce routeur virtuel uniquement, ou omettre l'option afin de voir les informations sur VRF sur tous les routeurs virtuels. Utilisez **show ospf ?** pour voir les options supplémentaires.
- **show bgp** [**vrf** *name* | **all**]

  Affiche les informations sur le processus BGP dans un routeur virtuel. Vous pouvez spécifier un routeur virtuel pour voir les informations sur le processus dans ce routeur virtuel uniquement, ou omettre l'option afin de voir les informations sur VRF sur tous les routeurs virtuels. Utilisez **show bgp ?** pour voir les options supplémentaires.
- **show eigrp** *option*

  Affiche les renseignements sur le processus EIGRP. Utilisez **show eigrp ?** pour voir les options disponibles.



CHAPITRE 14

Cartes de routage et autres objets pour le réglage du routage

Les différents protocoles de routage vous permettent d'affiner des activités telles que la distribution et l'agrégation des routes. Pour certaines fonctionnalités de réglage, vous utilisez des cartes de routage ou d'autres objets pour identifier les routes qui doivent être soumises à votre politique de réglage. Les cartes de routage ont la possibilité supplémentaire de définir des options sur les routes correspondantes, afin que vous puissiez apporter des modifications à la route que le routeur de saut suivant peut utiliser pour appliquer un comportement personnalisé.

La création de l'un de ces objets dépend de vos besoins pour affiner le comportement des protocoles de routage que vous mettez en œuvre. En évaluant d'abord vos besoins, vous déterminerez les types d'objets dont vous avez besoin pour la commande de réglage que vous souhaitez configurer.

- Configurer les cartes de routage, à la page 359
- Configurer une liste d'accès, à la page 365
- Configurer des listes d'accès AS Path, à la page 369
- Configurer des listes de la communauté, à la page 370
- Configurer les listes de politiques, à la page 373
- Configurer les listes de préfixe, à la page 375

Configurer les cartes de routage

Vous pouvez utiliser des cartes de routage à diverses fins, certains protocoles de routage prenant en charge plus d'utilisations que d'autres. L'utilisation la plus typique est d'affiner la redistribution des routes dans un autre protocole de routage.

Clauses d'autorisation et de refus des cartes de routage

Une carte de route comprend une ou plusieurs clauses **permit** ou **deny**. La séquence de ces clauses est importante : les routes sont évaluées par rapport à la carte de haut en bas, la première correspondance l'emporte. Si une route ne correspond à aucune clause, elle est considérée comme ne correspondant pas à la carte de route.

Chaque clause de permission peut contenir zéro ou plusieurs instructions **match** et **set**. L'instruction **match** détermine les routes qui correspondent à la clause, tandis que les instructions **set** modifient certaines caractéristiques des routes, telles que la métrique de route. Vous n'avez besoin d'aucune instruction set : vous

pouvez faire correspondre une voie de routage pour la redistribution (ou un autre service) sans modifier les routes de quelque façon que ce soit.

Chaque clause refuser peut contenir zéro ou plusieurs instructions de correspondance. Mais, comme les routes « refusées » ne correspondent tout simplement pas à la carte de route, il est inutile d'inclure des clauses « set », car l'action « set » ne peut pas être appliquée.

Instructions de correspondance et de définition de la carte de route

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 certains attributs des routes.

Pour chaque voie de routage qui est redistribuée, le routeur évalue d'abord les critères de correspondance d'une clause de la carte de route. Si la route correspond aux critères, la route est redistribuée ou rejetée comme indiqué par la clause d'autorisation ou de refus. Pour les correspondances avec les clauses d'autorisation, certains attributs de route peuvent être modifiés par les valeurs 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 route. 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. S'il n'y a aucune correspondance, le routage est considéré comme ne correspondant pas à la carte de route (équivalent à une action deny (refuser)).

Pour les instructions match et set dans une seule clause :

- Plusieurs instructions de correspondance sont associées à l'ET. C'est-à-dire qu'une voie de routage doit satisfaire à chaque instruction pour correspondre à la clause.
- Plusieurs valeurs dans une seule instruction de correspondance sont marquées OU. Autrement dit, si un routage correspond à une valeur dans cette instruction de correspondance, il est considéré comme correspondant à l'énoncé dans son ensemble.
- S'il n'y a aucune instruction de correspondance, toutes les routes correspondent à la clause.
- S'il n'y a aucune instruction set dans une clause d'autorisation de carte de route, la fonctionnalité (comme la redistribution) est appliquée à la route sans modification des attributs actuels de la route.
- Toutes les instructions set dans une clause de refus sont ignorées. Les routes « refusées » ne correspondent tout simplement pas à la carte de route, il est donc inutile d'inclure des clauses « set », car l'action « set » ne peut pas être appliquée.
- Une clause vide, une sans instruction match ou set, correspond à toutes les routes qui n'ont pas été correspondantes par les clauses précédentes. Par exemple :
  - Une clause d'autorisation vide permet une redistribution des routes restantes sans modification.
  - Une clause de refus vide ne permet pas la redistribution des routes restantes. Il s'agit de l'action par défaut si une carte de routage est complètement analysée, mais qu'aucune correspondance explicite n'est trouvée.

Configurer une carte de routage

Vous pouvez utiliser des cartes de routage à diverses fins, certains protocoles de routage prenant en charge plus d'utilisations que d'autres. L'utilisation la plus typique est d'affiner la redistribution des routes dans un autre protocole de routage.

Une carte de route comprend une ou plusieurs clauses **permit** ou **deny**. La séquence de ces clauses est importante : les routes sont évaluées par rapport à la carte de haut en bas, la première correspondance l'emporte. Si une route ne correspond à aucune clause, elle est considérée comme ne correspondant pas à la carte de route.

Chaque clause de permission peut contenir zéro ou plusieurs instructions **match** et **set**. L'instruction **match** détermine les routes qui correspondent à la clause, tandis que les instructions **set** modifient certaines caractéristiques des routes, telles que la métrique de route. Vous n'avez besoin d'aucune instruction set : vous pouvez faire correspondre une voie de routage pour la redistribution (ou un autre service) sans modifier les routes de quelque façon que ce soit.

Chaque clause refuser peut contenir zéro ou plusieurs instructions de correspondance. Mais, comme les routes « refusées » ne correspondent tout simplement pas à la carte de route, il est inutile d'inclure des clauses « set », car l'action « set » ne peut pas être appliquée.

Pour obtenir une explication détaillée de la façon dont les instructions match et set sont évaluées, lisez attentivement Instructions de correspondance et de définition de la carte de route, à la page 360.

Avant de commencer

Vous pouvez utiliser divers autres objets dans une carte de routage pour définir les critères de correspondance, tels que les listes d'accès, les listes d'accès de chemin de système autonome, les listes de communauté, les listes de politiques et les listes de préfixes. Vous devez créer ces objets avant de créer la carte de routage.

Pour la correspondance d'ACL, vous pouvez utiliser des listes de contrôle d'accès standard ou étendues pour les adresses IPv4, mais les listes de contrôle d'accès étendues uniquement pour IPv6. Comme les clauses de correspondance sont basées sur IPv4 ou IPv6 uniquement, assurez-vous que vos listes de contrôle d'accès ont le bon schéma d'adresses pour les instructions de correspondance.

Notez également que les critères de correspondance et d'ensemble sont différents pour BGP par rapport aux autres protocoles de routage. Assurez-vous de sélectionner les critères de correspondance ou d'ensemble appropriés pour le processus de routage qui utilisera la carte de routage.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Veuillez sélectionner **Smart CLI** > **Objects (Objets)** dans la table des matières.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Sélectionnez **Route Map** (Carte de routage) comme **CLI Template** (modèle CLI).

Étape 5 Saisissez un **nom** pour l'objet Smart CLI. Notez que ce nom est également saisi comme nom de carte de routage dans la première ligne du modèle d'interface de ligne de commande (dans la commande **route-map**).

Étape 6 Créez la première clause :

a) Cliquez sur la variable *de redistribution* et sélectionnez l'une des options suivantes :

- **permit**—Match (Mettre en correspondance). Les connexions qui correspondent à cette règle sont sélectionnées pour la fonctionnalité que vous configurez.
- **deny**—Do not match (Ne pas mettre en correspondance). Les connexions qui correspondent à cette règle sont exclues de la fonctionnalité. Notez que le trafic « refusé » n'est pas abandonné, il ne reçoit tout simplement pas le service qui lui est appliqué. Par exemple, si vous utilisez cette carte de routage pour définir les routes redistribuées, les espaces d'adresses « refusés » ne sont tout simplement pas redistribués.

b) Cliquez sur la variable **sequence-number** et saisissez le numéro de la clause, de 1 à 65 535.

Ce numéro est relatif aux autres clauses numérotées dans la carte de routage. Une pratique typique est d'ignorer le nombre par 10, c'est-à-dire 10, 20, 30, pour laisser la place d'insérer de nouvelles clauses ultérieurement.

Étape 7 Cliquez sur **Show Disabled** (Afficher les éléments désactivés) et configurez les instructions **match** pour la clause.

a) Cliquez sur le signe plus (+) à côté de la commande **configure** *clause* pour l'activer.

b) Cliquez sur *clause* et choisissez **bgp-match-clause** pour les cartes de routage BGP ou **match-clause** pour tous les autres protocoles de routage.

c) (Cartes de routage BGP.) Configurez n'importe quelle combinaison des instructions **match** suivantes pour identifier les routes spécifiques que vous ciblez dans cette clause. Assurez-vous de cliquer sur l'icône - pour désactiver les commandes que vous ne configurez pas.

- **match as-path**. Cliquez sur la variable et sélectionnez les objets AS Path qui définissent les numéros du système autonome à mettre en correspondance.
- **match community**. Cliquez sur la variable et sélectionnez les objets de liste de communautés qui définissent les communautés à mettre en correspondance.
- **match policy-list**. Cliquez sur la variable et sélectionnez les objets de liste de politiques qui définissent les critères de correspondance pour la clause.
- **match tag**. Cliquez sur la variable et saisissez la valeur de la balise de routage pour la mettre en correspondance, de 0 à 4 294 967 295.

d) (Tous les autres protocoles de routage.) Configurez n'importe quelle combinaison des instructions **match** suivantes pour identifier les routes spécifiques que vous ciblez dans cette clause. Assurez-vous de cliquer sur l'icône - pour désactiver les commandes que vous ne configurez pas. Vous devrez peut-être cliquer sur le signe + pour activer certaines de ces commandes.

- **match interface**. Cliquez sur la variable et sélectionnez toutes les interfaces dans les routes à mettre en correspondance.
- **configure match ipv4/ipv6 ip address** *list-type*. Activez la commande correcte pour votre version IP. Ensuite, cliquez sur la variable *list-type* et choisissez si vous souhaitez faire correspondre l'adresse IP dans la route en fonction de **access-list** ou **prefix-list**. Cela ajoutera une commande

match ipv4/ipv6 address, dans laquelle vous pouvez cliquer sur la variable et sélectionner les listes d'accès ou les listes de préfixes qui définissent les adresses IP à mettre en correspondance.

- **configure match ipv4/ipv6 ip next-hop** *list-type*. Cliquez sur la variable *la route en fonction* et choisissez si vous souhaitez faire correspondre l'adresse IP du routeur de saut suivant dans la route en fonction de **access-list** ou **prefix-list**. Cela ajoutera une commande **match ipv4/ipv6 next-hop**, dans laquelle vous pouvez cliquer sur la variable et sélectionner les listes d'accès ou les listes de préfixes qui définissent les adresses IP à mettre en correspondance.
- **configure match ipv4/ipv6 ip route-source** *list-type*. Cliquez sur la variable *la route en fonction* et choisissez si vous souhaitez faire correspondre l'adresse IP de la source de routage dans la route en fonction de **access-list** ou **prefix-list**. Cela ajoutera une commande **match ipv4/ipv6 route-source**, dans laquelle vous pouvez cliquer sur la variable et sélectionner les listes d'accès ou les listes de préfixes qui définissent les adresses IP à mettre en correspondance.
- **match metric**. Cliquez sur la variable et saisissez la mesure de routage pour la mettre en correspondance, de 1 à 4 294 967 295.
- **match route-type**. (OSPF, EIGRP.) Cliquez sur la variable et sélectionnez le type de routage :
  - **external-1**, **external-2**. Routes OSPF ou EIGRP externes de type 1 ou de type 2.
  - **internal**. Routes OSPF intra-zones et inter-zones ou routes internes EIGRP.
  - **local**. Routes BGP générées localement.
  - **nssa-external-1**, **nssa-external-2**. Routes externes de type 1 ou type 2 pour la zone Not So Stubby Area (NSSA).

Étape 8 (Facultatif, clauses d'autorisation uniquement.) Pour les routes autorisées, c'est-à-dire correspondantes, vous pouvez configurer les instructions **set** pour modifier les attributs de route. Vous n'avez pas besoin de modifier les routages ; par exemple, vous pouvez les redistribuer sans les modifier.

a) Cliquez sur **...** > **Duplicate** > **(Dupliquer)** à gauche de la commande configure match-clause ou **configure bgp-match-clause** dans la clause de permission. Une nouvelle commande **configure** *de clause* est ajoutée à la fin de la clause de permission.

b) Cliquez sur *clause* et choisissez **bgp-set-clause** ou **set-clause**, en fonction de ce que vous avez choisi pour la clause de correspondance.

c) (Cartes de routage BGP.) Configurez n'importe quelle combinaison des instructions **set** suivantes pour modifier les attributs des routes correspondantes. Assurez-vous de cliquer sur l'icône - pour désactiver les commandes que vous ne configurez pas.

- **configure set as-path** *options*. Cliquez sur *options* et sélectionnez **properties**, ce qui ajoute les commandes suivantes que vous devez configurer. En ajoutant des éléments aux chemins, même en dupliquant les numéros de système autonome, vous allongez le chemin et faites en sorte que la route soit moins susceptible d'être sélectionnée comme la meilleure route.
  - **set as-path prepend** *as-path*. Cliquez sur *as-path* et saisissez jusqu'à 10 numéros de système autonome à ajouter pour commencer l'attribut AS_PATH de la route. La modification s'applique aux cartes de routage BGP sortantes.
  - **set as-path prepend last-as** *value (valeur)*. Cliquez sur *value (valeur)* et saisissez le nombre de fois que le système doit faire précéder le numéro du système autonome du voisin de l'annonce au début de la variable AS_PATH. La modification s'applique aux cartes de routage BGP entrantes.

  - **set as-path tag**. Convertit la balise d'une route en chemin de système autonome. S'applique uniquement lors de la redistribution des routes dans BGP.

- **set community** *community-number (numéro de communauté) properties (propriétés)*. Cliquez sur *community-number* et saisissez la communauté pour le routage, de 1 à 4 694 967 295. Vous pouvez également cliquer sur *properties* (propriétés) et ajouter l'un des éléments suivants :
  - **internet** -- Les routes avec cette communauté sont annoncées à tous les homologues (internes et externes).
  - **no-advertise** -- Les routes avec cette communauté ne sont annoncées à aucun homologue (interne ou externe).
  - **no-export** -- Les routes avec cette communauté sont annoncées uniquement aux homologues du même système autonome ou aux autres systèmes sous-autonomes d'une confédération. Ces routes ne sont pas annoncées aux homologues externes.

- **set local-preference**. Cliquez sur la variable et saisissez une valeur de préférence pour le chemin d'accès au système autonome, de 0 à 4 294 967 295. Sauf si vous le modifiez dans les options de BGP globales, la préférence par défaut pour les routes de BGP est de 100. La route avec le numéro de préférence le plus élevé est préférée.
- **set weight**. Cliquez sur la variable et saisissez le poids pour le routage, de 0 à 65 535. Si le routeur détecte l'existence de plusieurs routes vers la même destination, la route ayant la pondération la plus élevée est préférée.
- **set origin** *options*. L'origine d'une route BGP est basée sur les informations de chemin de la route dans la table de routage IP principale. Vous pouvez le modifier en cliquant sur *options* et en sélectionnant la façon dont vous souhaitez définir le code d'origine BGP.
  - **igp**. Définissez l'origine sur le système distant de protocole de passerelle intérieure (IGP).
  - **incomplete**. Définissez l'origine comme Incomplete (Incomplète).

- **configure next-hop ipv4/ipv6** *options*. Il s'agit de commandes distinctes. Cliquez sur *options* pour la version IP appropriée et sélectionnez l'une des options suivantes. La définition de la passerelle du saut suivant est généralement quelque chose que vous faites lors de la mise en œuvre du routage basé sur les politiques.
  - **specific-ip**. Sélectionnez cette option si vous souhaitez définir explicitement l'adresse IP de la passerelle du saut suivant pour ce routage. La commande **set ip/ipv6 next-hop ip-address** est ajoutée. Cliquez sur la variable et saisissez l'adresse IP de la passerelle du saut suivant. Vous pouvez ajouter plusieurs adresses IP, séparées par un espace. Si l'adresse de la première passerelle est inaccessible, l'adresse suivante est essayée, et ainsi de suite.
  - **user-peer-address**. Sélectionnez cette option si vous souhaitez définir la passerelle du saut suivant comme adresse IP de l'homologue de BGP. Si vous utilisez cette option dans une carte de routage sortante d'un homologue BGP, le prochain saut des routes correspondantes annoncées sera défini sur l'adresse de peering du routeur local, ce qui désactive le calcul du prochain saut. Aucune configuration supplémentaire n'est requise pour cette commande.

- **set ipv4/ipv6 address** *prefix-list*. Il s'agit de commandes distinctes. Modifiez l'adresse IP de la route en fonction du contenu de la liste de préfixes que vous sélectionnez.
- **set automatic-tag**. Laissez le système calculer automatiquement une valeur de balise pour le routage.

d) (Tous les autres protocoles de routage.) Configurez n'importe quelle combinaison des instructions **set** suivantes pour modifier les attributs des routes correspondantes. Assurez-vous de cliquer sur l'icône - pour désactiver les commandes que vous ne configurez pas.

- **set metric**. Cliquez sur la variable et saisissez la valeur de la mesure, de 0 à 4 294 967 295. Cette valeur n'est pas utilisée par l'EIGRP.
- **set metric-type**. Cliquez sur la variable et sélectionnez le type de mesure :
  - **type-1**, **type-2**. Le type de route externe dans OSPF. Le type 2 est le paramètre par défaut.
  - **internal**. Définit la valeur de discriminateur de sortie multiple (MED) sur les préfixes annoncés aux voisins de BGP externes (eBGP) pour correspondre à la métrique du protocole de passerelle intérieure (IGP) du prochain saut de la route. Cela s'applique aux routes générées, dérivées de BGP internes (iBGP) et eBGP.

Étape 9 Ajoutez des clauses permit (autoriser) / deny (refuser) pour terminer la carte de routage.

Pour ajouter une clause, cliquez sur **...** > **Cliquez sur** > **Duplicate** > **(Dupliquer)** à gauche d'une ligne **permit** ou **deny**. Une nouvelle clause *de numéro de séquence de redistribution* est ajoutée immédiatement après la clause pour laquelle vous cliquez sur la commande Duplicate (Dupliquer).

Bien que les clauses de carte de routage soient évaluées dans l'ordre du numéro de séquence plutôt que dans l'ordre dans lequel elles apparaissent dans l'objet, il est plus facile de modifier votre objet si vous insérez de nouvelles clauses dans l'ordre séquentiel. Vous ne pouvez pas déplacer les clauses dans l'objet.

Notez que la duplication d'une clause insère simplement une nouvelle clause vide, sans caractéristiques préconfigurées. Après avoir créé le « dupliquer », procédez comme expliqué ci-dessus pour le configurer selon vos besoins.

Étape 10 Cliquez sur **OK** pour enregistrer l'objet.

Vous pouvez maintenant utiliser l'objet dans une configuration de processus de routage ou dans un objet FlexConfig, pour une fonctionnalité qui nécessite une carte de routage.

Configurer une liste d'accès

Un objet de liste d'accès, également appelé liste de contrôle d'accès (ACL ou access control list), sélectionne le trafic auquel un service s'appliquera. Vous utilisez ces objets lors de la configuration de fonctionnalités particulières, telles que pour les cartes de routage. Le trafic identifié comme autorisé par la liste de contrôle d'accès (ACL) reçoit le service, tandis que le trafic « bloqué » est exclu du service. L'exclusion du trafic d'un service ne signifie pas nécessairement son abandon.

Vous pouvez configurer les types d'ACL suivants :

- Étendu : identifie le trafic en fonction de l'adresse et des ports source et destination. Les adresses IPv4 et IPv6 sont prises en charge.
- Standard : le trafic est identifié en fonction de l'adresse de destination uniquement. Seulement IPv4 est pris en charge.

Une ACL est composée d'une ou de plusieurs entrées de contrôle d'accès (ACE), ou règles. L'ordre des ACE est important. Lors de l'évaluation de la liste de contrôle d'accès pour déterminer si un paquet correspond à une entrée ACE « autorisée », le paquet est testé par rapport à chaque ACE dans l'ordre dans lequel les entrées sont répertoriées. Une fois qu'une correspondance est trouvée, aucune autre Ace n'est vérifiée. Par exemple, si vous souhaitez faire correspondre 10.100.10.1 mais exclure le reste de 10.100.10.0/24, l'entrée d'autorisation pour 10.100.10.1 doit se trouver avant l'entrée de refus pour 10.100.10.0/24. En général, placez des règles plus spécifiques en haut d'une liste de contrôle d'accès.

Les paquets qui ne correspondent pas à une entrée d'autorisation sont considérés comme refusés ou exclus de la correspondance.

Les rubriques suivantes expliquent comment configurer les objets ACL.

Configurer les listes de contrôle d'accès étendues.

Utilisez des objets ACL étendus lorsque vous souhaitez faire correspondre le trafic en fonction des adresses de source et de destination, du protocole et du port, ou s'il s'agit du trafic IPv6.

Avant de commencer

Créez tous les objets de réseau ou de port dont vous aurez besoin dans les ACE que vous créez dans l'objet.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Veuillez sélectionner **Smart CLI** > **Objects (Objets)** dans la table des matières.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Sélectionnez **Extended Access List** (Liste de contrôle d'accès étendue) comme **modèle CLI**.

Étape 5 Saisissez un **Name** (Nom) pour l'objet Smart CLI. Notez que ce nom est également utilisé comme nom d'ACL dans la première ligne du modèle CLI (dans la commande **access list**).

Étape 6 Créez l'ACE qui doit être la règle supérieure dans l'ACL.

Chaque liste de commandes contenues dans une seule commande **configure access list entry** est essentiellement une commande ACE, bien qu'une fois déployée, le système peut décomposer la commande en une série d'ACE, en particulier si vous incluez plusieurs objets réseau.

a) Dans la commande d'entrée de liste de configuration d'accès, cliquez sur *Action* et sélectionnez l'une des options suivantes :

- **permit** : match (Mettre en correspondance). Les connexions qui correspondent à cette ACE sont sélectionnées pour la fonctionnalité que vous configurez.

- **deny**—Ne pas mettre en correspondance. Les connexions qui correspondent à cette entrée ACE sont exclues de la fonctionnalité. Notez que le trafic « refusé » n'est pas abandonné, il ne reçoit tout simplement pas le service qui lui est appliqué. Par exemple, dans une carte de routage, si vous utilisez cette liste de contrôle d'accès pour définir les routes redistribuées, les espaces d'adresses « refusés » ne sont tout simplement pas redistribués.

b) Dans la commande **permit/deny network**, cliquez sur les variables pour sélectionner les objets réseau qui définissent l'adresse IP source et l'adresse IP de destination de la connexion. Vous pouvez sélectionner plusieurs objets. Pour spécifier l'adresse « any » (toute), sélectionnez les objets any-ipv4 et any-ipv6.

L'objet ou le groupe d'objets ne peut pas contenir de nom de domaine complet (FQDN) : les objets doivent préciser uniquement les adresses IP. Les objets FQDN sont valides dans les règles de contrôle d'accès uniquement.

c) Dans la commande **configure permit/deny port**, cliquez sur *Options* et sélectionnez l'une des options suivantes, ce qui ajoutera la commande permit (autoriser) ou deny (refuser) correspondante au modèle :

- **any**—Si le port n'a pas d'importance. C'est-à-dire que vous faites correspondre n'importe quel type de trafic IP.
- **any-source** — si le port TCP/UDP source n'a pas d'importance, mais que vous souhaitez préciser le port de destination. Cliquez sur la variable *destination-port* dans la commande **permit/deny port** et sélectionnez l'objet de port.
- **any-destination** — si le port TCP/UDP de destination n'a pas d'importance, mais que vous souhaitez préciser le port source. Cliquez sur la variable *source-port* dans la commande **permit/deny port** et sélectionnez l'objet de port.
- **source-destination** — si les ports TCP/UDP source et de destination sont importants. Cliquez sur les variables *source-port* et *destination-port* dans la commande **permit/deny port** et sélectionnez les objets de port.

d) Dans la commande **configure logging**, sélectionnez **disabled**. La journalisation s'applique aux listes de contrôle d'accès, et vous ne pouvez pas utiliser ces objets pour le contrôle d'accès. Ainsi, les options de journalisation sont ignorées, quelle que soit votre sélection.

Étape 7 Ajoutez des ACE pour terminer l'ACL.

Pour ajouter une commande ACE, cliquez sur **…** > **Duplicate** > **(Dupliquer)** à gauche de la ligne **configure access list entry**. Un nouveau groupe ACE est ajouté immédiatement après l'ACE pour lequel vous cliquez sur la commande Dupliquer.

Ainsi, lorsque vous avez plusieurs ACE dans l'objet, choisissez avec soin quelle ACE vous « dupliquez ». Vous ne pouvez pas déplacer les ACE dans l'objet. Par conséquent, si vous faites une erreur, vous devez recréer manuellement l'ACE au bon emplacement.

Notez que la duplication d'une ACE insère simplement une nouvelle ACE vide, sans caractéristiques préconfigurées. Après avoir créé le « dupliquer », procédez comme expliqué ci-dessus pour le configurer selon vos besoins.

Étape 8 Cliquez sur **OK** pour enregistrer l'objet.

Vous pouvez maintenant utiliser l'objet dans un objet de carte de routage ou dans un objet FlexConfig, pour une fonctionnalité qui nécessite une liste de contrôle d'accès étendue.

Configurer les listes d'accès standard

Utilisez les objets ACL standard lorsque vous souhaitez mettre en correspondance le trafic en fonction de l'adresse IPv4 de destination uniquement, et que la fonctionnalité que vous configurez prend en charge les ACL standard. Sinon, utilisez des listes de contrôle d'accès étendues.

Avant de commencer

Créez tous les objets réseau dont vous aurez besoin dans les ACE que vous créez dans l'objet.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Veuillez sélectionner **Smart CLI** > **Objects (Objets)** dans la table des matières.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Sélectionnez **Standard Access List** (Liste d'accès standard) comme **CLI Template** (Modèle CLI).

Étape 5 Saisissez un **Name** (Nom) pour l'objet Smart CLI. Notez que ce nom est également utilisé comme nom d'ACL dans la première ligne du modèle CLI (dans la commande **access list**).

Étape 6 Créez l'ACE qui doit être la règle supérieure dans l'ACL.

Chaque liste de commandes contenues dans une seule commande **configure action** correspond à une commande ACE.

a) Dans la commande **configure action**, cliquez sur *action* et sélectionnez l'une des options suivantes :

- **permit** : match (Mettre en correspondance). Les connexions qui correspondent à cette ACE sont sélectionnées pour la fonctionnalité que vous configurez.
- **deny**—Ne pas mettre en correspondance. Les connexions qui correspondent à cette entrée ACE sont exclues de la fonctionnalité. Notez que le trafic « refusé » n'est pas abandonné, il ne reçoit tout simplement pas le service qui lui est appliqué. Par exemple, dans une carte de routage, si vous utilisez cette liste de contrôle d'accès pour définir les routes redistribuées, les espaces d'adresses « refusés » ne sont tout simplement pas redistribués.

b) Dans la commande **permit/deny host**, cliquez sur la variable pour sélectionner l'objet réseau qui définit l'adresse IP de destination de la connexion. L'objet peut préciser une adresse de réseau ou d'hôte. Vous pouvez sélectionner un objet par commande **permit/deny host** ; cliquez sur **…** > **Cliquez sur** > **Duplicate** > **(Dupliquer)** dans la commande pour préciser d'autres adresses, qui deviendront des ACE distinctes avec la même action. Pour spécifier une adresse « any » (tout), sélectionnez l'objet any-ipv4.

Étape 7 Ajoutez des ACE pour terminer l'ACL.

Pour ajouter une commande ACE, cliquez sur **…** > **Duplicate** > **(Dupliquer)** à gauche de la ligne **configure action**. Un nouveau groupe ACE est ajouté immédiatement après l'ACE pour lequel vous cliquez sur la commande Dupliquer.

Ainsi, lorsque vous avez plusieurs ACE dans l'objet, choisissez avec soin quelle ACE vous « dupliquez ». Vous ne pouvez pas déplacer les ACE dans l'objet. Par conséquent, si vous faites une erreur, vous devez recréer manuellement l'ACE au bon emplacement.

Notez que la duplication d'une ACE insère simplement une nouvelle ACE vide, sans caractéristiques préconfigurées. Après avoir créé le « dupliquer », procédez comme expliqué ci-dessus pour le configurer selon vos besoins.

Étape 8 Cliquez sur **OK** pour enregistrer l'objet.

Vous pouvez maintenant utiliser l'objet dans un objet de carte de routage ou dans un objet FlexConfig, pour une fonctionnalité qui nécessite une liste de contrôle d'accès standard.

Configurer des listes d'accès AS Path

Vous pouvez utiliser une liste d'accès AS Path pour filtrer les mises à jour de voisin BGP en fonction des numéros de système autonome dans les mises à jour. Les mises à jour des numéros de système autonomes acceptés sont acceptées, tandis que celles des numéros de système autonomes refusés sont rejetées, c'est-à-dire qu'elles ne sont pas ajoutées à la table de routage.

Vous pouvez également appliquer le filtrage de chemin AS dans le sens sortant et filtrer les mises à jour que vous envoyez aux voisins.

En outre, vous pouvez utiliser des objets de chemin AS dans les cartes de routage pour l'agrégation des adresses BGP,

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Veuillez sélectionner **Smart CLI** > **Objects (Objets)** dans la table des matières.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Sélectionnez **ASPath** (Entrée de chemin de système autonome) comme **CLI Template** (Modèle CLI).

Étape 5 Saisissez un **Name** (Nom) pour l'objet Smart CLI. Le nom doit être un nombre dans la plage de 1 à 500. Notez que ce nom est également saisi comme nom de liste d'accès de chemin de système autonome dans la première ligne du modèle d'interface de ligne de commande (dans la commande **as-path**).

Étape 6 Configurez une entrée de chemin de système autonome.

Chaque entrée est contenue sur une seule ligne à partir de l'option *Action*.

a) Cliquez sur *Action* et sélectionnez l'une des options suivantes :

- **permit**—Match (Mettre en correspondance). Les connexions qui correspondent à cette règle sont sélectionnées pour la fonctionnalité que vous configurez.
- **deny**—Do not match (Ne pas mettre en correspondance). Les connexions qui correspondent à cette règle sont exclues de la fonctionnalité. Notez que le trafic « refusé » n'est pas abandonné, il ne reçoit tout simplement pas le service qui lui est appliqué. Par exemple, dans une carte de routage, si vous utilisez cet objet pour définir les routes redistribuées, les espaces d'adresses « refusés » ne sont tout simplement pas redistribués.

b) Cliquez sur *regex*, puis saisissez l'expression régulière qui définit les numéros de système autonome devant correspondre à cette entrée.

Dans sa forme la plus simple, l'expression régulière est simplement un numéro de chemin de système autonome complet, et vous autorisez ou refusez les mises à jour de route à partir d'un seul système autonome.

Le numéro de système autonome peut être compris entre 1 et 4294967295 ou entre 1.0 et 6553565535. Le numéro de système autonome est une valeur attribuée de façon unique qui identifie chaque réseau sur Internet. Le système prend en charge les notations asplain et asdot, telles que définies dans la RFC 5396. La notation que vous devez utiliser dépend de l'activation de la commande **bgp asnotation dot** dans les paramètres globaux de BGP.

Étape 7 Ajoutez des entrées pour terminer la liste d'accès de chemin de système autonome.

Pour ajouter une entrée, cliquez sur **....** > **Duplicate** > **(Dupliquer)** à gauche de la ligne *action*. Une nouvelle entrée est ajoutée immédiatement après celle pour laquelle vous cliquez sur la commande Duplicate (Dupliquer).

Ainsi, lorsque vous avez de nombreuses entrées dans l'objet, choisissez soigneusement celle que vous souhaitez « dupliquer ». Vous ne pouvez pas déplacer les entrées dans l'objet ; si vous faites une erreur, vous devez recréer l'entrée au bon emplacement. Les règles sont évaluées de haut en bas, la première correspondance l'emporte.

Notez que la duplication d'une entrée insère simplement une nouvelle entrée vide, sans caractéristiques préconfigurées. Après avoir créé le « dupliquer », procédez comme expliqué ci-dessus pour le configurer selon vos besoins.

Étape 8 Cliquez sur **OK** pour enregistrer l'objet.

Vous pouvez maintenant utiliser l'objet dans un objet BGP, un objet de carte de routage ou un objet FlexConfig, pour une fonctionnalité qui nécessite une liste d'accès de chemin AS.

Configurer des listes de la communauté

Si vous activez votre processus BGP pour envoyer des informations de communauté, vous pouvez utiliser les listes de communautés comme clause de correspondance dans les cartes de routage afin de définir les attributs des routes correspondantes. Par exemple, vous pouvez modifier les préférences de routage pour certaines communautés.

Une communauté est un attribut ou une étiquette facultatif qu'un fournisseur de services associerait aux routages annoncés pour un groupe de destinations qui partagent un attribut commun. Les numéros de communauté spécifiques seraient quelque chose que votre fournisseur de services Internet pourrait annoncer : vous devrez obtenir les numéros et leur signification de votre fournisseur de services Internet, puis choisir la façon dont vous souhaitez les gérer à l'aide d'une carte de routage.

Les listes de communautés sont ordonnées et les correspondances sont déterminées selon une méthode de haut en bas, le premier résultat l'emporte, similaire aux listes d'accès et de préfixes.

Il existe deux types de liste de communauté :

- Standard : utilisez une liste standard lorsque vous souhaitez cibler des communautés bien connues, comme celles obtenues auprès de votre fournisseur de services.
- Expanded (Étendue) : utilisez une liste étendue lorsque vous souhaitez mettre en correspondance un ensemble de communautés en fonction d'expressions régulières.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Veuillez sélectionner **Smart CLI** > **Objects (Objets)** dans la table des matières.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Sélectionnez **Standard Community List** (Liste de communauté standard) ou **Expanded Community List** (Liste de communauté étendue) comme **CLI Template** (Modèle CLI).

Étape 5 Saisissez un **Name** (nom) pour l'objet Smart CLI. Notez que ce nom est également saisi comme Community List name (nom de liste de communauté) dans la première ligne du modèle CLI (dans la commande **community-list**).

Étape 6 (Liste standard.) Configurez une entrée de liste de communauté.

Chaque entrée est contenue sur une seule ligne à partir de l'option *Action*.

a) Cliquez sur *Action* et sélectionnez l'une des options suivantes :

- **permit**—Match (Mettre en correspondance). Les connexions qui correspondent à cette règle sont sélectionnées pour la fonctionnalité que vous configurez.
- **deny**—Do not match (Ne pas mettre en correspondance). Les connexions qui correspondent à cette règle sont exclues de la fonctionnalité. Notez que le trafic « refusé » n'est pas abandonné, il ne reçoit tout simplement pas le service qui lui est appliqué. Par exemple, dans une carte de routage, si vous utilisez cette règle pour définir les routes redistribuées, les espaces d'adresses « refusés » ne sont tout simplement pas redistribués.

b) Cliquez sur *community-number* (numéro de communauté) et saisissez jusqu'à 10 communautés séparées par des espaces. Plusieurs communautés sur une seule règle sont utilisées dans le protocole ET, de sorte qu'une correspondance n'existe que si toutes les communautés correspondent dans la route.

Saisissez la communauté au format décimal (1-4294967295) ou en format AA:NN (chaque valeur est de 1 à 66535) en fonction de la méthode de numérotation activée pour votre processus BGP. Obtenez ces chiffres auprès de votre fournisseur de services Internet ou d'autres voisins BGP.

c) (Facultatif) Cliquez sur *properties* (propriétés) et ajoutez d'autres communautés bien connues à la règle.

- **internet** -- Les routes avec cette communauté sont annoncées à tous les homologues (internes et externes).
- **no-advertise** -- Les routes avec cette communauté ne sont annoncées à aucun homologue (interne ou externe).
- **no-export** -- Les routes avec cette communauté sont annoncées uniquement aux homologues du même système autonome ou aux autres systèmes sous-autonomes d'une confédération. Ces routes ne sont pas annoncées aux homologues externes.

Étape 7 (Liste étendue.) Configurez une entrée de liste de communauté.

a) Cliquez sur *action* et sélectionnez **permit** ou **deny**. Ces actions sont expliquées ci-dessus.
b) Cliquez sur *regex* (expression régulière) et saisissez l'expression régulière qui définit les communautés qui doivent correspondre à cette entrée.

L'ordre de mise en correspondance à l'aide du caractère * ou + est la structure la plus longue en premier. Les constructions imbriquées sont mises en correspondance de l'extérieur vers l'intérieur. Les constructions concaténées sont évaluées à partir du côté gauche. Si une expression régulière peut correspondre à deux parties d'une même chaîne, elle correspondra d'abord à la partie la plus ancienne. Pour plus d'informations sur l'écriture d'expressions régulières, consultez l'annexe « Expressions régulières » du Guide de configuration des services de terminaux Cisco IOS.

Étape 8 Ajoutez des entrées pour terminer la liste de communautés.

Pour ajouter une entrée, cliquez sur **...** > **Duplicate**(Dupliquer) à gauche de la ligne *action*. Une nouvelle entrée est ajoutée immédiatement après celle pour laquelle vous cliquez sur la commande Duplicate (Dupliquer).

Ainsi, lorsque vous avez de nombreuses entrées dans l'objet, choisissez soigneusement celle que vous souhaitez « dupliquer ». Vous ne pouvez pas déplacer les entrées dans l'objet ; si vous faites une erreur, vous devez recréer l'entrée au bon emplacement.

Notez que la duplication d'une entrée insère simplement une nouvelle entrée vide, sans caractéristiques préconfigurées. Après avoir créé le « dupliquer », procédez comme expliqué ci-dessus pour le configurer selon vos besoins.

Étape 9 Cliquez sur **OK** pour enregistrer l'objet.

Vous pouvez maintenant utiliser l'objet dans une carte de routage, un processus de routage, ou un objet FlexConfig pour une fonctionnalité nécessitant une liste de communautés.

Configurer les listes de politiques

Vous pouvez utiliser les listes de politiques dans les cartes de routage en remplacement d'une ou de plusieurs clauses de correspondance. Ainsi, si vous avez un ensemble de clauses de correspondance que vous souhaitez réutiliser, une carte de routage simplifie votre configuration, de sorte que vous n'avez pas besoin de répéter les clauses de correspondance dans chaque carte de routage. Vous pouvez utiliser des cartes de routage qui font référence à des listes de politiques dans BGP.

Dans une carte de routage, vous pouvez inclure d'autres clauses de correspondance en plus des listes de politiques. Les clauses de correspondance de la liste de politiques correspondent uniquement aux attributs entrants.

Les listes de politiques prennent uniquement en charge la mise en correspondance des adresses IPv4; vous ne pouvez pas mettre en correspondance les adresses IPv6.

Pour les clauses de correspondance dans la carte de politiques :

- Les clauses de correspondance multiples sont associées à l'ET. C'est-à-dire qu'une voie de routage doit satisfaire à chaque clause pour correspondre à la liste des politiques.
- Plusieurs valeurs dans une seule clause de correspondance sont marquées OU. Autrement dit, si un routage correspond à une valeur dans cette instruction de correspondance, il est considéré comme correspondant à l'énoncé dans son ensemble.

Avant de commencer

Si vous configurez des clauses de correspondance pour les listes d'accès, les listes de préfixes ou les listes d'accès de chemin de système autonome, vous devez créer ces objets avant de créer la liste de politiques.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Veuillez sélectionner **Smart CLI** > **Objects (Objets)** dans la table des matières.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Sélectionnez **Policy List** (Liste de politiques) comme **CLI Template** (Modèle CLI).

Étape 5 Saisissez un **nom** pour l'objet Smart CLI. Notez que ce nom est également saisi comme nom de liste de politiques dans la première ligne du modèle d'interface de ligne de commande (dans la commande **policy-list**).

Étape 6 Cliquez sur *action* dans la commande **policy-list**, sélectionnez l'une des options suivantes :

- **permit** : match (Mettre en correspondance). Les connexions qui correspondent à cette liste sont sélectionnées pour la fonctionnalité que vous configurez.

- **deny**—Do not match (Ne pas mettre en correspondance). Les connexions qui correspondent à cette liste sont exclues de la fonctionnalité. Notez que le trafic « refusé » n'est pas abandonné, il ne reçoit tout simplement pas le service qui lui est appliqué. Par exemple, dans une carte de routage, si vous utilisez cet objet pour définir les routes redistribuées, les espaces d'adresses « refusés » ne sont tout simplement pas redistribués.

Étape 7 Cliquez sur **Show Disabled** (Afficher désactivé) au-dessus du modèle pour afficher les commandes de correspondance. Vous devez cliquer sur l'icône + à gauche des instructions de correspondance que vous souhaitez activer. Configurez n'importe quelle combinaison des instructions de correspondance suivantes pour définir les routes que vous ciblez.

- **match as-path**. Cliquez sur la variable et sélectionnez les objets AS Path qui définissent les numéros du système autonome à mettre en correspondance.
- **configure match ip address** *list-type*. Cliquez sur la variable *list-type* et choisissez si vous souhaitez faire correspondre l'adresse IP dans le routage en fonction de **access-list** ou **prefix-list**. Cela ajoutera une commande **match ip address**, dans laquelle vous pouvez cliquer sur la variable et sélectionner les listes d'accès standard ou les listes de préfixes IPv4 qui définissent les adresses IP à mettre en correspondance.
- **configure match ip next-hop** *list-type*. Cliquez sur la variable *la route en fonction* et choisissez si vous souhaitez faire correspondre l'adresse IP du routeur de saut suivant dans la route en fonction de **access-list** ou **prefix-list**. Cela ajoutera une commande **match ip next-hop**, dans laquelle vous pouvez cliquer sur la variable et sélectionner les listes d'accès standard ou les listes de préfixes IPv4 qui définissent les adresses IP à mettre en correspondance.
- **configure match ip route-source** *list-type*. Cliquez sur la variable *la route en fonction* et choisissez si vous souhaitez faire correspondre l'adresse IP de la source de routage dans la route en fonction de **access-list** ou **prefix-list**. Cela ajoutera une commande **match ip route-source**, dans laquelle vous pouvez cliquer sur la variable et sélectionner les listes d'accès standard ou les listes de préfixes IPv4 qui définissent les adresses IP à mettre en correspondance.
- **match community** *community-list options*. Cliquez sur la variable *community-list* et sélectionnez les objets de liste de communauté qui définissent les communautés à mettre en correspondance. Si vous souhaitez que les routes correspondent à la liste de communautés uniquement si toutes les communautés de la liste sont mises en correspondance, cliquez sur *options* et sélectionnez **exact-match**.
- **match interface**. Cliquez sur la variable et sélectionnez toutes les interfaces dans les routes à mettre en correspondance.
- **match metric**. Cliquez sur la variable et saisissez la mesure de discriminateur de sortie multiple (MED) de routage pour la mettre en correspondance, de 1 à 4 294 967 295.
- **match tag**. Cliquez sur la variable et saisissez la valeur de la balise de routage pour la mettre en correspondance, de 0 à 4 294 967 295.

Étape 8 Cliquez sur **OK** pour enregistrer l'objet.

Vous pouvez maintenant utiliser l'objet dans un objet de carte de routage pour une utilisation dans le routage BGP.

Configurer les listes de préfixe

Les listes de préfixes sont similaires aux listes de contrôle d'accès. Une liste de préfixes est une liste ordonnée de règles d'autorisation/refus, où l'autorisation indique les préfixes d'adresse qui doivent correspondre à la liste et le refus indique les préfixes d'adresse qui ne doivent pas correspondre à la liste. Le système évalue les correspondances de haut en bas et attribue l'action en fonction de la première règle mise en correspondance, et pas nécessairement de la règle la mieux adaptée. Vous devez donc spécifier avec soin les numéros de séquence pour vous assurer d'obtenir les correspondances dont vous avez besoin.

Vous pouvez utiliser des listes de préfixes pour le filtrage OSPF ou les cartes de routage BGP, OSPF ou EIGRP pour la redistribution ou l'injection de route, ou pour le filtrage de voisin BGP.

Il existe des listes de préfixes distinctes pour les adresses IPv4 et IPv6, mais la structure des listes est la même.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Veuillez sélectionner **Smart CLI** > **Objects (Objets)** dans la table des matières.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Sélectionnez **IPv4 Prefix List** (Liste des préfixes IPv4) ou **IPv6 Prefix List** (Liste des préfixes IPv6) comme **CLI Template** (modèle CLI).

Étape 5 Saisissez un **nom** pour l'objet Smart CLI. Notez que ce nom est également saisi comme nom de liste de préfixes dans la première ligne du modèle CLI (dans la commande) **prefix-list**).

Étape 6 Configurez une entrée de liste de préfixes à l'aide de la ligne de commande **seq**.

Chaque entrée figure sur une seule ligne qui commence par l'option **seq**.

a) Dans **seq**, cliquez sur *sequence-number (numéro de séquence)* et saisissez le numéro pour cette règle, de 1 à 4 294 967 294. Le nombre est relatif aux numéros de séquence des autres règles, 1 étant la première règle évaluée. La pratique courante consiste à incrémenter par pas de 5, c'est-à-dire 5, 10, 15, etc. Cela vous permet d'insérer de nouvelles règles sans avoir à modifier les numéros de séquence des autres règles.

b) Cliquez sur *Action* et sélectionnez l'une des options suivantes :

- **permit**—Match (Mettre en correspondance). Les connexions qui correspondent à cette règle sont sélectionnées pour la fonctionnalité que vous configurez.
- **deny**—Do not match (Ne pas mettre en correspondance). Les connexions qui correspondent à cette règle sont exclues de la fonctionnalité. Notez que le trafic « refusé » n'est pas abandonné, il ne reçoit tout simplement pas le service qui lui est appliqué. Par exemple, dans une carte de routage, si vous utilisez cette règle pour définir les routes redistribuées, les espaces d'adresses « refusés » ne sont tout simplement pas redistribués.

c) Cliquez sur *ip-address-mask* (adresse IP et masque) et saisissez l'adresse réseau et le masque (au format CIDR pour IPv4) ou la longueur de préfixe pour IPv6. Par exemple, 10.100.10.0/24 (IPv4) ou 2001:DB8:0:CD30::/60 (IPv6).

Le système utilise une correspondance exacte pour cette adresse ou ce masque, sauf si vous incluez également l'une des options **ge** ou **le**. Par exemple, 10.100.10.10/8 ne correspond pas à 10.100.10.0/24, sauf si vous incluez **ge 9** dans la règle.

La longueur du masque ou du préfixe peut être :

- IPv4 = 0 à 32
- IPv6 = 0 à 128

d) (Facultatif) Vous pouvez utiliser les mots-clés **ge** et **le** pour préciser la plage de longueur de préfixe à mettre en correspondance pour les préfixes plus spécifiques que l'adresse IP et la longueur de masque ou de préfixe. Sans ces mots-clés, seules les correspondances exactes sont prises en compte pour correspondre à la règle.

ge *min-prefix-length* spécifie la longueur minimale du préfixe à mettre en correspondance. La valeur doit être supérieure à la longueur du masque et inférieure ou égale à la longueur maximale de préfixe, si elle est spécifiée dans l'option **le**.

le *max-prefix-length* spécifie la longueur maximale du préfixe à mettre en correspondance. La valeur doit être supérieure ou égale à la longueur minimale du préfixe, le cas échéant, ou supérieure à la longueur du masque si la longueur minimale du préfixe n'est pas précisée.

Outre les limites de longueur relative mentionnées ci-dessus, les longueurs dans ces options ont les limites externes suivantes :

- IPv4 = 1 à 32
- IPv6 = 0 à 128

Étape 7 Ajoutez des entrées pour terminer la liste des préfixes.

Pour ajouter une entrée, cliquez sur **....** > **Duplicate** > **(Dupliquer)** à gauche d'une ligne **seq**. Une nouvelle entrée est ajoutée immédiatement après celle pour laquelle vous cliquez sur la commande Duplicate (Dupliquer).

Pour votre commodité, il est préférable d'essayer de conserver les entrées dans l'ordre de séquence. Cependant, une fois déployée, la liste des préfixes sera réécrite dans l'ordre séquentiel, même si vous les avez mélangées dans l'objet.

Notez que la duplication d'une entrée insère simplement une nouvelle entrée vide, sans caractéristiques préconfigurées. Après avoir créé le « dupliquer », procédez comme expliqué ci-dessus pour le configurer selon vos besoins.

Étape 8 Cliquez sur **OK** pour enregistrer l'objet.

Vous pouvez maintenant utiliser l'objet dans une carte de route, un processus de routage, ou un objet FlexConfig, pour une fonctionnalité qui nécessite une liste de préfixes.

Exemples

Voici quelques exemples sur la façon de mettre en correspondance les préfixes à l'aide d'une liste de préfixes. Le numéro de séquence est omis des exemples pour des raisons de simplicité. Le comportement réel de chaque règle est modifié par toute règle antérieure dans la séquence qui correspond à un sous-ensemble des espaces d'adresse couverts.

- Rejeter la route par défaut 0.0.0.0/0 :

```
refuser 0.0.0.0/0
```

- Autoriser le préfixe 10.0.0.0/8 :

```
autoriser 10.0.0.0/8
```

- Autoriser une longueur de masque pouvant atteindre 24 bits dans les routes avec le préfixe 192/8 :

```
autoriser 192.168.0.0/8 le 24
```

- Refuser les longueurs de masque supérieures à 25 bits dans les routes avec un préfixe 192/8 :

```
refuser 192.168.0.0/8 ge 25
```

- Autoriser les longueurs de masque de 8 à 24 bits dans tous les espaces d'adresse :

```
autoriser 0.0.0.0/0 ge 8 le 24
```

- Refuser les longueurs de masque supérieures à 25 bits dans tous les espaces d'adresse :

```
refuser 0.0.0.0/0 ge 25
```

- Refuser toutes les routes avec le préfixe 10/8 :

```
refuser 10.0.0.0/8 le 32
```

- Refuser tous les masques d'une longueur supérieure à 25 bits pour les routes ayant un préfixe de 192.168.1/24 :

```
refuser 192.168.1.0/24 ge 25
```

- Autoriser toutes les routes avec un préfixe de 0/0 :

```
autoriser 0.0.0.0/0 le 32
```



CHAPITRE 15

Open Shortest Path First (OSPF)

OSPF (Open Shortest Path First) est un protocole de passerelle intérieure à état de liaison. Les routeurs OSPF diffusent les informations d'état de liaison aux routeurs voisins afin que tous les routeurs d'une zone OSPF disposent d'une vue complète de la topologie du réseau.

Il existe des versions d'OSPF distinctes en fonction de la version IP : OSPFv2 pour les réseaux IPv4 et OSPFv3 pour les réseaux IPv6. Ces versions sont indépendantes ; autrement dit, OSPFv3 ne remplace pas OSPFv2.

Vous pouvez configurer OSPFv2 à l'aide d'objets Smart CLI afin d'intégrer votre périphérique à la topologie de réseau OSPFv2. Vous ne pouvez pas configurer OSPFv3.

- Configurer le processus et les zones OSPFv2, à la page 379
- Personnalisation des caractéristiques du processus OSPF et des zones, à la page 381
- Configurer les paramètres de l'interface OSPFv2 et l'authentification OSPF, à la page 395
- Supervision OSPF, à la page 399

Configurer le processus et les zones OSPFv2

Vous pouvez configurer jusqu'à 2 processus OSPFv2 en utilisant Firepower Threat Defense. Les numéros de processus sont uniquement des indicateurs internes ; ils n'ont pas besoin de correspondre aux numéros de processus utilisés sur d'autres périphériques, bien que vous puissiez rendre les chiffres cohérents pour vos propres besoins de suivi.

Si vous utilisez la numérotation de réseau privé, comme 192.168.1.0/24, pour tous les réseaux internes, vous devrez peut-être séparer les adresses privées des adresses publiques, en utilisant un processus OSPFv2 pour ces réseaux internes et un deuxième processus pour les réseaux externes, réseaux publics adressables. 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. 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.

Les numéros de zone, en revanche, existent dans le réseau et vous devez utiliser les mêmes numéros que ceux utilisés par les autres routeurs adjacents. Si vous configurez un réseau à zone unique, utilisez la zone 0, également connue sous le nom de zone de réseau fédérateur. Pour les réseaux à zones multiples, où vous avez une conception de réseau hiérarchique, vous devez comprendre les zones définies dans le réseau et savoir à quelles zones ce périphérique est censé participer.

Si vous utilisez des routeurs virtuels, vous pouvez configurer 2 processus OSPFv2 par routeur virtuel.

La procédure suivante explique comment créer un processus OSPFv2 unique. Répétez la procédure pour créer un deuxième processus.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez OSPF.

Étape 3 Cliquez sur l'onglet **OSPF**.

Étape 4 Effectuez l'une des opérations suivantes :

- Pour créer un processus, cliquez sur le signe plus **(+)** ou cliquez sur le bouton **Create OSPF Object**(Créer un objet OSPF).
- Cliquez sur l'icône de modification ( ) de l'objet que vous souhaitez modifier. Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Si vous n'avez plus besoin d'un processus, cliquez sur l'icône de la corbeille pour supprimer l'objet.

Étape 5 Entrez un nom pour l'objet et, facultativement, une description.

Étape 6 Configurez les propriétés de base du processus :

- **router ospf** *process-id*. Cliquez sur *process-id* et saisissez un nombre compris entre 1 et 65535. Ce numéro n'a de signification que dans cet appareil et n'a pas besoin de correspondre aux numéros de processus configurés sur d'autres routeurs. Le numéro doit être unique dans un routeur virtuel.
- **log-adj-changes** *log-state*. Cliquez sur *log-state* et sélectionnez l'une des options suivantes :
  - **enable** (conseillé) : le système génère un message syslog lorsqu'un voisin OSPFv2 monte ou tombe en panne. Si vous sélectionnez cette option, une ligne **log-adj-changes** *log-type* supplémentaire est ajoutée à l'objet. Cliquez sur *log-type* et sélectionnez **detail** si vous souhaitez générer un message syslog pour chaque changement d'état, pas seulement lorsqu'un voisin monte ou tombe en panne.

    Si vous ne souhaitez pas de messages détaillés, laissez simplement *log-type* comme option. Ne supprimez pas cette ligne de l'objet.
  - **disable** : aucun message syslog n'est généré. La ligne **no log-adj-changes** est ajoutée à l'objet : ne supprimez pas cette ligne.

Étape 7 Cliquez sur le lien **Show Disabled** (Afficher les éléments désactivés) au-dessus du corps de l'objet pour ajouter toutes les autres lignes de configuration possibles.

Étape 8 Configurez le numéro de zone.

a) Cliquez sur le **+** à gauche de la ligne **area** *area-id* pour activer la commande. Vous ne pouvez pas configurer une commande avant de l'activer.

b) Cliquez sur *area-id* et saisissez le numéro de la zone. Ce numéro de zone doit être le même que celui utilisé par les autres routeurs qui définissent la zone OSPFv2. Vous pouvez spécifier l'ID de zone sous la forme d'un nombre décimal ou d'une adresse IP. Les valeurs décimales valides vont de 0 à 4294967295.

Étape 9 Configurez les réseaux et les interfaces qui doivent être acheminés dans la zone.

a) Cliquez sur le + à gauche de la ligne **configure area** *area-id options*.
b) Cliquez sur *area-id* et saisissez le même numéro de zone dans la commande **area**.
c) Cliquez sur *options* et sélectionnez **properties**. Cette action ajoute plusieurs lignes, dont une activée par défaut, la commande **network**.
d) Dans la commande **network**, cliquez sur *network-object* et sélectionnez l'objet qui définit un réseau à inclure dans cette zone. En règle générale, il s'agirait d'un réseau directement connecté. Par exemple, si l'adresse IP de l'interface interne est 192.168.1.1/24, l'objet réseau associé à cette commande contiendra 192.168.1.0/24. Si l'objet n'existe pas encore, cliquez sur **Create New Network** (Créer un nouveau réseau) pour le créer maintenant.
e) (Facultatif) Dans la commande **network**, cliquez sur *tag-interface (interface de balise)* et sélectionnez l'interface qui héberge ou achemine vers le réseau. Si vous sélectionnez l'interface, le système peut vous empêcher de modifier l'adresse sur l'interface, car elle est utilisée dans le processus de routage. Cela vous aide à vous rappeler que toute modification de l'adressage d'interface peut avoir une incidence sur votre configuration de routage.

   Si vous sélectionnez une interface ici, avant de pouvoir modifier l'adresse sur une interface, vous devez d'abord la supprimer du processus de routage. Ensuite, après avoir modifié l'adresse IP, n'oubliez pas de revenir ici et de sélectionner les nouveaux réseaux et la nouvelle interface pour vous assurer d'un processus de routage correctement configuré.

f) Toutes les autres nouvelles lignes de zone sont facultatives et désactivées par défaut. Configurez-les uniquement si vous avez besoin de ces services. Pour en savoir plus, consultez Personnalisation des caractéristiques du processus OSPF et des zones, à la page 381.

Étape 10 Si vous configurez le processus pour un réseau à zones multiples, passez le curseur sur la zone à gauche des lignes encerclées - sur les lignes **area** et **configure area** et cliquez sur **...** > **dupliquer**. Configurez ensuite la nouvelle zone et ses réseaux comme expliqué ci-dessus. Répétez ce processus jusqu'à ce que vous ayez défini toutes les zones auxquelles ce processus de routage doit participer.

Étape 11 Cliquez sur **OK**.

Personnalisation des caractéristiques du processus OSPF et des zones

OSPF comprend de nombreuses options qui ont des valeurs par défaut. Ces valeurs fonctionnent bien pour de nombreux réseaux. Cependant, vous devrez peut-être ajuster un ou plusieurs paramètres pour obtenir le comportement précis dont vous avez besoin. Les rubriques suivantes expliquent les différentes façons de personnaliser votre processus de routage OSPFv2.

Configurer les paramètres avancés pour un processus OSPF

Vous pouvez configurer plusieurs paramètres qui contrôlent le comportement global d'un processus OSPFv2, notamment les mesures de distance, les minuteurs, le redémarrage progressif et l'ID de routeur utilisé pour envoyer des annonces d'état de liaison et d'autres mises à jour de routage. Les paramètres avancés comprennent des paramètres par défaut appropriés pour la plupart des réseaux.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez OSPF.

Étape 3 Cliquez sur l'onglet **OSPF**.

Étape 4 Ajoutez ou modifiez un objet de processus OSPF.

Étape 5 Recherchez la ligne **setup ospf**.

Lors de l'ajout d'un objet, vous devez cliquer sur le lien **Show Disabled** (Afficher les éléments désactivés) pour voir la ligne. Ensuite, cliquez sur le **signe plus (+)** pour la commande afin de l'activer, puis cliquez sur *configuration* et sélectionnez **advanced**. Les commandes qui seront activées par défaut sont déjà activées avec leurs valeurs par défaut.

Lors de la modification d'un objet, la ligne sera déjà activée.

Pour le reste de cette procédure, vous devez cliquer sur **« Show Disabled » (Afficher les éléments désactivés)**. Si vous ne pouvez pas voir une commande, assurez-vous d'exposer les commandes désactivées.

Étape 6 (Facultatif) Configurez l'ID du routeur.

Cliquez sur le **signe plus (+)** pour activer la commande **router-id**, puis cliquez sur la variable et saisissez l'adresse IPv4 qui doit être utilisée lors de l'envoi des mises à jour de routeur à partir de ce périphérique. Deux routeurs dans un système OSPF ne peuvent pas avoir le même ID de routeur. Assurez-vous donc qu'il est unique dans la zone.

Si vous ne spécifiez pas explicitement d'ID de routeur pour le processus, le système utilise l'adresse IP la plus élevée attribuée à une interface active. Ainsi, l'ID du routeur peut changer si vous désactivez l'interface sélectionnée ou si vous modifiez ses adresses. En attribuant explicitement un ID de routeur, vous assurez la cohérence de votre processus.

Étape 7 (Facultatif) Configurez la compatibilité RFC 1583 lors du calcul des coûts récapitulatifs de route.

Cliquez sur + pour activer la commande **configure summary-route-cost**, puis cliquez sur la variable et sélectionnez soit **any**, ce qui désactive la compatibilité RFC 1583, soit **rfc1583**, ce qui l'active.

Même si cette commande n'est pas activée par défaut dans l'objet OSPF, la compatibilité avec la RFC 1583 est en fait la méthode par défaut utilisée lors du calcul des coûts récapitulatifs de la route. Si vous examinez la configuration définie dans l'interface de ligne de commande, seul le paramètre désactivé s'affiche.

Des boucles de routage peuvent se produire lorsque la compatibilité RFC 1583 est activée. Désactivez-la pour éviter les boucles de routage. Assurez-vous de définir la compatibilité RFC 1583 de la même manière sur tous les routeurs OSPF dans un domaine de routage OSPF.

Étape 8 (Facultatif) Supprimez les messages de journal système pour les annonces d'état de liaison (LSA) de multidiffusion OSPF (MOSPF).

Cliquez sur + pour activer la commande **ignore lsa mospf**.

Le système ne prend pas en charge les paquets LSA de type 6 MOSPF. Vous pouvez activer cette commande pour que le système n'envoie pas de messages de journal système lorsqu'il reçoit ces paquets, afin de réduire le bruit dans votre serveur de journaux système.

Étape 9 Configurez les mesures de distance.

Les commandes **distance** suivantes sont activées par défaut. Vous pouvez modifier les distances administratives de route OSPF en fonction du type de route. Les distances sont de 1 à 255, les nombres les plus élevés étant moins fiables que les nombres inférieurs. Ces mesures sont utilisées pour évaluer la valeur relative d'une route apprise lors de la comparaison de routes similaires de différents processus.

- **distance ospf inter-area 110**. Cliquez sur le numéro et définissez la distance pour toutes les routes d'une zone à une autre zone.
- **distance ospf intra-area 110**. Cliquez sur le numéro et définissez la distance pour toutes les routes à l'intérieur d'une zone.
- **distance ospf external 110**. Cliquez sur le numéro et définissez la distance pour les routes des autres domaines de routage apprises par la redistribution.

Étape 10 Configurez les minuteurs de calcul de route pour le processus OSPF.

Les commandes de minuterie suivantes sont activées avec ces valeurs par défaut.

- **timers lsa arrival 1000**. Cliquez sur le nombre et définissez l'intervalle minimal auquel le système accepte la même publicité d'état de liaison (LSA) des voisins OSPF, de 0 à 600 000 millisecondes. Utilisez cette commande pour indiquer l'intervalle minimal qui doit s'écouler entre l'acceptation d'un même LSA provenant de voisins. Les LSA qui arrivent avant ce délai minimal sont ignorés.
- **timers pacing flood 33**. Cliquez sur le numéro et définissez l'intervalle auquel les LSA de la file d'attente d'inondation sont cadencés entre les mises à jour, de 5 à 100 millisecondes.
- **timers pacing lsp-group 240**. Cliquez sur le numéro et définissez l'intervalle auquel les annonces d'état de liaison (LSA) OSPF sont collectées dans un groupe et sont actualisées, contrôlées ou vieillies, de 10 à 1 800 secondes.
- **timers pacing retransmission 66**. Cliquez sur le numéro et définissez l'intervalle de temps auquel les LSA dans la file d'attente de retransmission sont cadencées, de 5 à 200 millisecondes. Nous vous recommandons de ne pas modifier la minuterie de retransmission des paquets tant que toutes les autres options pour répondre aux exigences d'injection de paquets OSPF n'ont pas été épuisées. Plus précisément, configurez la summarisation, l'utilisation des zones stub, le réglage des files d'attente et le réglage des tampons avant de modifier les minuteurs d'inondation par défaut.
- **timers throttle lsa 0 5000 5000**. Cliquez sur les numéros et définissez les valeurs de limitation de débit pour la génération des annonces d'état de liaison (LSA) du protocole Open Shortest Path First (OSPF). La limitation des LSA et SPF fournit un mécanisme dynamique pour retarder les mises à jour de LSA dans OSPF pendant les périodes d'instabilité du réseau et permettre une convergence OSPF plus rapide. Les valeurs possibles sont les suivantes :
  - **Intervalle de début** (premier nombre) : délai minimal pour générer la première occurrence d'un LSA, de 1 à 600 000 millisecondes. La première instance de LSA est générée immédiatement après un changement de topologie OSPF local. Le LSA suivant est généré uniquement après cet intervalle de début. Précisez 0 pour que les LSA soient générés sans délai.
  - **Hold Time** (temps d'attente) (deuxième nombre) : délai minimal avant de générer de nouveau le LSA, de 1 à 600 000 millisecondes. Cette valeur sert à calculer les délais de limitation de débit ultérieurs pour la génération de LSA.
  - **Maximum Interval** (Intervalle maximal) (troisième nombre) : délai maximal avant de générer de nouveau le LSA, de 1 à 600000 millisecondes.

- **timers throttle spf 5000 10000 10000**. Cliquez sur les numéros et définissez les valeurs de limitation de débit pour la génération du premier chemin le plus court (SPF). Les valeurs possibles sont les suivantes :
  - **Start Interval** (Intervalle de début) (premier nombre) : délai avant la prise en compte d'une modification du calcul SPF, de 1 à 600 000 millisecondes.
  - **Hold Time** (Temps d'attente) (deuxième nombre) : délai entre le premier et le deuxième calculs SPF, de 1 à 600 000 millisecondes.
  - **Maximum Interval** (Intervalle maximal) (troisième nombre) : temps d'attente maximal pour les calculs SPF, de 1 à 600 000 millisecondes.

Étape 11 (Facultatif) Générez une route externe par défaut dans un domaine de routage OSPF.

Cliquez sur + pour activer la commande **default-information originate**. Vous pouvez éventuellement activer et configurer les commandes suivantes pour affiner la fonctionnalité :

- **default-information originate always**. Annoncez toujours une route par défaut même s'il n'y a pas de route par défaut.
- **default-information originate metric 1 metric-type** *metric-type-value*. Le type de métrique et la valeur utilisés pour générer la route par défaut.
  - Cliquez sur le numéro **metric** et saisissez la valeur de la mesure OSPF par défaut, de 0 à 16 777 214. Sauf si vous savez que vous avez besoin d'une valeur différente, saisissez 10.
  - Cliquez sur le numéro **metric-type** et sélectionnez 1 ou 2 comme type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPF. La valeur par défaut est 2.
- **default-information originate route-map** *route-map*. Sélectionnez une route-map qui précise le processus de routage qui génère la route par défaut lorsque les conditions de la route-map sont satisfaites.

Étape 12 (Facultatif) Configurez le redémarrage progressif de la transmission sans arrêt (NSF) si le périphérique est configuré pour la haute disponibilité (HA).

Le système 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. Cette capacité est utile en cas de défaillance d'un composant (par exemple, en haute disponibilité, l'unité active bascule vers l'unité de secours; ou, dans une grappe, l'unité principale échoue et une unité secondaire est élue nouvelle unité principale), ou lorsqu'une mise à niveau logicielle transparente est planifiée.

Vous pouvez configurer le redémarrage progressif sur OSPFv2 en utilisant NSF IETF (RFC 3623).

Vous pouvez configurer un périphérique comme compatible NSF (NSF-capable) ou NSF-aware. Un périphérique compatible NSF peut indiquer ses propres activités de redémarrage aux voisins, et il peut aider un voisin qui redémarre.

- Vous pouvez configurer un périphérique comme NSF-aware, quel que soit son mode de fonctionnement.
- Un périphérique doit être en mode haute disponibilité (basculement) ou en mode grappe EtherChannel étendu (L2) pour être configuré comme compatible NSF.

Remarque
Vous ne devez pas configurer le processus OSPF pour utiliser des paquets Hello rapides si vous configurez également le redémarrage progressif. Le redémarrage progressif ne peut pas se produire avec les paquets Hello

rapides, car le temps nécessaire au changement de rôle entre les unités active et de secours est supérieur à l'intervalle mort configuré.

Pour configurer le redémarrage progressif

a) Cliquez sur + pour activer la commande **configure nsf graceful-restart**.
b) Cliquez sur *mechanism (mécanisme)* et sélectionnez l'une des options suivantes :
   - **cisco** pour configurer un périphérique compatible NSF conformément aux RFC 4811 et RFC 4812 de Cisco.
   - **ietf** pour configurer un périphérique compatible NSF conformément à la RFC 3623 de l'IETF.
   - **both** pour configurer le périphérique comme assistant NSF-aware plutôt que comme périphérique compatible NSF.
   - **none** pour désactiver le redémarrage progressif si vous l'avez déjà configuré.
c) Votre sélection à l'étape précédente ajoute les commandes nécessaires pour mettre en œuvre le redémarrage progressif selon vos spécifications. Ne désactivez pas ces commandes. Il n'y a qu'une seule commande qui nécessite éventuellement une configuration supplémentaire. Voici une explication des commandes ajoutées. Une variante de la commande **no** désactive la fonctionnalité associée.
   - **nsf cisco helper**. Activer le mode assistant de transfert sans arrêt Cisco (NSF). Lorsque le périphérique Firewall Threat Defense compatible NSF effectue un redémarrage progressif, les périphériques Firewall Threat Defense de l'assistant contribuent au processus de récupération du transfert sans arrêt Cisco.
   - **nsf ietf helper** *mode-option*. Activer le mode assistant de transfert sans arrêt IETF (NSF). Lorsque le périphérique Firewall Threat Defense compatible NSF effectue un redémarrage progressif, les périphériques Firewall Threat Defense de l'assistant contribuent au processus de récupération du transfert sans arrêt Cisco. Vous pouvez également cliquer sur *mode-option* (option de mode) et activer la vérification stricte des annonces d'état de liaison (LSA). Lorsque la vérification stricte des LSA est activée, le système assistant met fin au processus d'assistance du système en cours de redémarrage s'il détecte une modification d'un LSA qui serait propagée vers ce système, ou si un LSA modifié figure sur la liste de retransmission du système en cours de redémarrage lors de l'initiation du redémarrage progressif.
   - **capability lls**. Active la signalisation locale de liaison (LLS), nécessaire au redémarrage progressif Cisco.
   - **capability opaque**. Active les annonces d'état de liaison (LSA) sombres, ce qui est nécessaire pour le redémarrage progressif IETF.

Étape 13 Cliquez sur **OK**.

Configurer les propriétés de la zone OSPF

Vous pouvez configurer plusieurs paramètres de zone OSPF. Vous pouvez définir les réseaux à annoncer dans la zone, ainsi que le filtrage et les liens virtuels. En outre, ces paramètres de zone incluent 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.

Lorsque vous configurez les paramètres de zone, vous devez savoir comment le système fonctionne dans la zone.

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 du LSA ABR de type 3 vous permet d'avoir des zones privée et publique distinctes, le système agissant comme un 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.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez OSPF.

Étape 3 Cliquez sur l'onglet **OSPF**.

Étape 4 Ajoutez ou modifiez un objet de processus OSPF.

Étape 5 Configurez le numéro de zone.

a) Cliquez sur le **+** à gauche de la ligne **area** *area-id* pour activer la commande. Vous ne pouvez pas configurer une commande avant de l'activer.

b) Cliquez sur *area-id* et saisissez le numéro de la zone. Ce numéro de zone doit être le même que celui utilisé par les autres routeurs qui définissent la zone OSPFv2. Vous pouvez spécifier l'ID de zone sous la forme d'un nombre décimal ou d'une adresse IP. Les valeurs décimales valides vont de 0 à 4294967295.

Étape 6 Configurez les réseaux et les interfaces qui doivent être acheminés dans la zone.

a) Cliquez sur le **+** à gauche de la ligne **configure area** *area-id options*.

b) Cliquez sur *area-id* et saisissez le même numéro de zone dans la commande **area**.

c) Cliquez sur *options* et sélectionnez **properties**. Cette action ajoute plusieurs lignes, dont une activée par défaut, la commande **network**.

d) Dans la commande **network**, cliquez sur *network-object* et sélectionnez l'objet qui définit un réseau à inclure dans cette zone. En règle générale, il s'agirait d'un réseau directement connecté. Par exemple, si l'adresse IP de l'interface interne est 192.168.1.1/24, l'objet réseau associé à cette commande contiendra 192.168.1.0/24. Si l'objet n'existe pas encore, cliquez sur **Create New Network** (Créer un nouveau réseau) pour le créer maintenant.

e) (Facultatif) Dans la commande **network**, cliquez sur *tag-interface (interface de balise)* et sélectionnez l'interface qui héberge ou achemine vers le réseau. Si vous sélectionnez l'interface, le système peut vous empêcher de modifier l'adresse sur l'interface, car elle est utilisée dans le processus de routage. Cela vous aide à vous rappeler que toute modification de l'adressage d'interface peut avoir une incidence sur votre configuration de routage.

Si vous sélectionnez une interface ici, avant de pouvoir modifier l'adresse sur une interface, vous devez d'abord la supprimer du processus de routage. Ensuite, après avoir modifié l'adresse IP, n'oubliez pas de revenir ici et de sélectionner les nouveaux réseaux et la nouvelle interface pour vous assurer d'un processus de routage correctement configuré.

Étape 7 (Facultatif) Configurez le coût de la route récapitulative par défaut envoyée à une zone de talon ou à une zone pas si bornée (NSSA).

Cette option n'est significative que si vous configurez la zone pour qu'elle soit un talon ou NSSA, comme expliqué ci-dessous. Cliquez sur **+** pour activer la commande suivante dans les propriétés de la zone :

area *zone-id* **default-cost 1**

Si nécessaire, saisissez le bon ID de zone. Ensuite, cliquez sur le nombre et saisissez le coût relatif du routage, de 0 à 16777214. La valeur par défaut est 1. Plus le nombre est élevé, moins la route sera utilisée sur une autre route qui s'applique à la destination.

Étape 8 (Facultatif) Configurez le filtrage de préfixe pour la zone.

Vous pouvez filtrer les préfixes annoncés dans les annonces d'état de liaison (LSA) de type 3 entre les zones OSPFv2 d'un routeur de frontière de zone (ABR). Le filtrage de préfixes améliore votre contrôle de la distribution des routages entre les zones OSPF. Avec le filtrage de préfixes, vous pouvez autoriser uniquement l'envoi de préfixes spécifiques d'une zone à une autre et restreindre tous les autres préfixes. Vous pouvez appliquer ce type de filtrage de zone hors d'une zone OSPF spécifique, dans une zone OSPF spécifique ou à la fois vers et depuis la même zone OSPF.

Avant de configurer cette commande, vous devez créer les listes de préfixes, qui sont des objets Smart CLI, sur la page **Device** > **Advanced Configuration** (Configuration avancée du périphérique). Vous pouvez configurer des listes de préfixes distinctes pour les annonces entrantes ou sortantes : sélectionnez la direction pour le paramètre de direction de filtre.

area *zone-id* **filter-list prefix** *prefix-list filter-direction*

Étape 9 (Facultatif) Configurez la zone en tant que zone tampon.

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. Vous devez utiliser le routage par défaut dans la zone tampon pour qu'il fonctionne correctement. Pour réduire davantage le nombre de LSA envoyés dans une zone tampon, vous pouvez utiliser le mot-clé **no-summary** de la commande **area stub** sur l'ABR pour l'empêcher d'envoyer une annonce récapitulative de lien (LSA de type 3) dans la zone tampon.

Pour configurer la zone en tant que zone tampon :

a) Cliquez sur le signe plus **+** à gauche de la ligne area-id configurée comme type.
b) Cliquez sur le *type* et sélectionnez **stub**. Cela ajoutera la commande de zone tampon après la ligne de configuration.
c) Éventuellement, dans la commande **area stub**, cliquez sur *tub-parameters (paramètres de zone tampon)* et sélectionnez **no-summary**.

Étape 10 (Facultatif) Configurez la zone en tant que zone pas si dense (NSSA).

Une zone pas si dense (NSSA) est semblable à une zone tampon. 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 traduits en LSA de type 5 par les routeurs ABR, qui sont inondés dans l'ensemble du domaine de routage. La récapitulation et le filtrage sont pris en charge pendant la traduction.

Vous pouvez simplifier l'administration si vous êtes un fournisseur de services Internet ou un administrateur réseau qui doit connecter un site central à l'aide d'OSPFv2 à un site distant qui utilise un protocole de routage différent en exécutant la zone de connexion en tant que NSSA. La connexion entre le routeur de frontière du site d'entreprise et le routeur distant ne peut pas être exécutée en tant que zone tampon OSPFv2, car les routes du site distant ne peuvent pas être redistribuées dans la zone tampon, ce qui signifie que deux protocoles de

routage devront être maintenus. Un protocole simple tel que RIP est généralement exécuté pour gérer 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.

Pour configurer la zone en tant que NSSA :

a) Cliquez sur le bouton + à gauche de la ligne **setup** *area-id* **as** *de type*.
b) Cliquez sur le *type* et sélectionnez **nssa**. Cela ajoutera plusieurs commandes après la ligne de configuration, y compris la commande **area nssa**, que vous devez laisser activée.
c) (Facultatif) Pour générer une route par défaut de type 7 dans le NSSA, cliquez sur le bouton + pour activer la commande suivante :

   area *area-id* **nssa default-information-originate metric 1 metric-type 2**

   Vous pouvez éventuellement ajuster les valeurs suivantes :

   - Cliquez sur le numéro **metric** et saisissez la valeur de la mesure OSPF par défaut, de 0 à 16 777 214. Sauf si vous savez que vous avez besoin d'une valeur différente, saisissez 10.
   - Cliquez sur le numéro **metric-type** et sélectionnez 1 ou 2 comme type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPF. La valeur par défaut est 2.

d) (Facultatif) Si le système est un ABR et que vous souhaitez une redistribution à partir d'autres protocoles de routage pour importer les routes dans les zones normales uniquement et non dans le NSSA, cliquez sur le bouton+ pour activer la commande suivante :

   area *area-id* **nssa no-redistribution**

e) (Facultatif) Si vous ne souhaitez pas injecter de routes récapitulatives dans le NSSA, cliquez sur le bouton + pour activer la commande suivante :

   area *area-id* **nssa no-summary**

Étape 11 (Facultatif) Configurez les liens virtuels pour la zone.

Dans OSPF, toutes les zones doivent être connectées à une zone de réseau fédérateur. En cas de perte de la connexion au réseau fédérateur, vous pouvez la réparer en établissant une liaison virtuelle. Vous pouvez configurer des liens virtuels vers les routeurs connectés à la zone de réseau fédérateur.

a) Cliquez sur le bouton + à gauche de la ligne **configure area** *area-id* **virtual-link** *d'option ip_address*.
b) Cliquez sur *ip_address* et saisissez l'ID du routeur avec lequel vous établissez la liaison virtuelle.
c) (Facultatif) Cliquez sur *option* et sélectionnez **properties** pour ajuster les attributs suivants, qui ont tous des valeurs par défaut appropriées à la plupart des réseaux. La première partie de ces commandes est omise, car il ne s'agit que de paramètres sur la même commande :

   - **authentication** *auth-type*. Cliquez sur + pour activer la commande, puis cliquez sur *auth-type* et sélectionnez **none**, **password**, ou **message-digest**. Configurez les options de clé si vous sélectionnez autre chose que aucune. Les options sont les mêmes que celles que vous configurez sur une interface

OSPF, comme expliqué dans Configurer les paramètres de l'interface OSPFv2 et l'authentification OSPF, à la page 395. Configurez l'authentification uniquement si l'autre routeur utilise l'authentification.

- **hello-interval 10**. Cliquez sur le nombre et saisissez l'intervalle entre les paquets Hello envoyés sur l'interface, de 1 à 65535 secondes.
- **retransmit-interval 5**. Cliquez sur le nombre et saisissez le délai entre les retransmissions de LSA pour la liaison virtuelle, de 1 à 65535 secondes.
- **transmit-delay 1**. Cliquez sur le nombre et saisissez le délai entre le moment où OSPF reçoit un changement de topologie et le moment où il démarre un calcul SPF (court le plus court chemin), de 0 à 65535 secondes.

d) Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **configure area virtual-link** pour définir une autre liaison virtuelle. Définissez-en autant que vous le souhaitez.

Étape 12 (Facultatif) Si le système est un routeur de frontière de zone (ABR), configurez des plages pour regrouper ou résumer les routes pour la zone.

Lorsque vous configurez la commande **area range**, le résultat est qu'une seule route récapitulative est annoncée à d'autres zones par l'ABR. Les informations de routage sont condensées aux limites de la zone. À l'extérieur de la zone, une seule voie de routage est annoncée pour chaque plage d'adresses. Ce comportement s'appelle récapitulation de route. Vous pouvez configurer plusieurs commandes **area range** pour une zone. De cette manière, OSPF peut résumer les adresses pour de nombreux ensembles différents de plages d'adresses.

Pour configurer la récapitulation des routes

a) Cliquez sur le signe **+** à gauche de la ligne **area** *area-id* **range** *paramètres de plage d'objets de réseau*.
b) Cliquez sur *network-object* (objet réseau) et sélectionnez l'objet réseau qui définit la plage d'adresses dont vous souhaitez résumer les routes.
c) (Facultatif) Cliquez sur *range-parameters* (paramètres de plage) et sélectionnez l'un des attributs suivants :

- **advertise**. Définit l'état de la plage d'adresses à annoncer et génère des annonces récapitulatives d'état de liaison (LSA) de type 3. Il s'agit de l'option par défaut si vous ne sélectionnez aucune option.
- **not-advertise**. Définit l'état de la plage d'adresses à DoNotAdvertise. Le LSA récapitulatif de type 3 est supprimé et les réseaux composants restent masqués par les autres réseaux.

d) Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **area range** pour définir une autre récapitulation de route. Définissez-en autant que vous le souhaitez.

Étape 13 Si vous configurez le processus pour un réseau multi-zone, passez le curseur sur la zone à gauche des lignes encerclées - sur les lignes **area** et **configure area**, puis cliquez sur **...** > **Dupliquer**. Configurez ensuite la nouvelle zone, ses réseaux et les autres paramètres, comme expliqué ci-dessus. Répétez ce processus jusqu'à ce que vous ayez défini toutes les zones auxquelles ce processus de routage doit participer.

Étape 14 Cliquez sur **OK**.

Configurer les voisins OSPF statiques

Vous devez définir des voisins OSPF statiques pour annoncer les routes OSPF sur un réseau point à point de non-diffusion, c'est-à-dire un tunnel VPN.

Vous n'avez pas besoin de définir les voisins statiques qui se trouvent sur des réseaux de diffusion classiques, car ces routeurs peuvent établir eux-mêmes des relations d'adjacence.

Avant de commencer

Déterminez l'interface par laquelle le système doit atteindre le voisin. Vous devez configurer les paramètres OSPF de cette interface avant de pouvoir définir le routeur voisin.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez OSPF.

Étape 3 Cliquez sur l'onglet **OSPF**.

Étape 4 Ajoutez ou modifiez l'objet d'interface OSPF et activez la commande **ospf network point-to-point non-broadcast** pour l'interface sélectionnée. Enregistrez vos modifications.

Étape 5 Ajoutez ou modifiez un objet de processus OSPF.

Étape 6 Cliquez sur **Show Disabled** (Afficher désactivé) pour exposer toutes les commandes, puis cliquez sur **+** pour activer la commande **neighbor**.

Étape 7 Configurez l'adresse du voisin.

neighbor *adresse IP* **interface** *interface*

- Cliquez sur *ip-address* et saisissez l'adresse IP du routeur voisin.
- Cliquez sur *interface* et sélectionnez l'interface par laquelle le système peut atteindre le routeur.

Étape 8 Si nécessaire, configurez une route statique pour le routeur voisin.

Si l'adresse IP du routeur se trouve sur le même réseau que l'interface sélectionnée, une route statique n'est pas nécessaire. Par exemple, si vous sélectionnez une interface dont l'adresse IP est 10.100.10.1/24, et l'adresse du voisin est 10.100.10.2/24, vous n'avez pas besoin de route statique.

Étape 9 Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **neighbor** pour définir un autre voisin statique. Définissez-en autant que vous le souhaitez.

Étape 10 Cliquez sur **OK**.

Configurer les adresses de résumé OSPF

Lorsque les routages d'autres protocoles sont redistribués dans OSPF, chaque routage est annoncée individuellement dans un LSA externe. Cependant, vous pouvez configurer le système pour annoncer une seule route pour toutes les routes redistribuées qui sont incluses pour une adresse et un masque de 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.

Le récapitulatif de route consiste à regrouper les adresses annoncées. 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.

Avant de commencer

Créez des objets réseau pour toutes les adresses que vous souhaitez résumer.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez OSPF.

Étape 3 Cliquez sur l'onglet **OSPF**.

Étape 4 Ajoutez ou modifiez un objet de processus OSPF.

Étape 5 Cliquez sur **Show Disabled (**Afficher désactivé) pour exposer toutes les commandes, puis cliquez sur **+** pour activer la commande **configure** *network-object* **as** *option* **summary-address**.

Étape 6 Cliquez sur *network-object* et sélectionnez l'objet qui définit l'espace d'adresse que vous souhaitez résumer.

Étape 7 Cliquez sur *option* et sélectionnez l'une des options suivantes :

- **advertising**. Annoncez les routes qui correspondent à l'adresse.
- **non-advertising**. Supprimez les routes qui correspondent à l'adresse.

Étape 8 (Facultatif) Pour ajouter une valeur de balise au routage résumé, cliquez sur **+** pour activer la commande **summary-address tag**, cliquez sur la variable *de numéro de balise* et saisissez le numéro de balise, de 0 à 4294967295.

Cette valeur n'est pas utilisée par OSPF lui-même. Elle peut être utilisée pour communiquer des informations entre les routeurs de limite de système autonome (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 (0) est utilisé.

La raison principale d'utiliser les valeurs de balise est de contrôler la redistribution en fonction du numéro de balise. Si vous ne l'utilisez pas dans vos cartes de routage de redistribution, il n'est pas nécessaire de le configurer ici.

Étape 9 Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **configure summary-address** pour définir une autre récapitulation de route. Définissez-en autant que vous le souhaitez.

Étape 10 Cliquez sur **OK**.

Configurer les règles de filtre OSPF

Créez les objets de liste d'accès standard de l'interface de ligne de commande Smart dont vous avez besoin pour chaque règle de filtre. Utilisez les entrées de contrôle d'accès (ACE) pour filtrer les routages qui correspondent à l'entrée et autorisez les ACE pour les routes qui doivent être mises à jour.

Avant de commencer

Vous pouvez configurer des filtres LSA de type 3 pour les routeurs de frontière de zone (ABR) afin de permettre uniquement l'envoi de préfixes spécifiés d'une zone à une autre et de restreindre tous les autres préfixes. Vous pouvez appliquer ce type de filtrage de zone hors d'une zone OSPF spécifique, dans une zone OSPF spécifique ou à la fois vers et depuis la même zone OSPF. Le filtrage LSA OSPF ABR de type 3 améliore votre contrôle de la distribution des routages entre les zones OSPF.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez OSPF.

Étape 3 Cliquez sur l'onglet **OSPF**.

Étape 4 Ajoutez ou modifiez un objet de processus OSPF.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) pour exposer toutes les commandes, puis cliquez sur **+** pour activer la commande **configure filter-rules** *direction*.

Étape 6 Cliquez sur *direction* et sélectionnez **in**, pour filtrer les mises à jour entrantes, ou **out**, pour filtrer les mises à jour sortantes.

Étape 7 Pour les filtres entrants, vous pouvez éventuellement spécifier l'interface sur laquelle filtrer les mises à jour. Si vous ne spécifiez pas d'interface, le filtre s'applique à toutes les mises à jour reçues sur n'importe quelle interface.

a) Cliquez sur **+** pour activer la commande **distribute-list** *acl-name* **in interface** *interface*.

b) Cliquez sur la variable *interface* et sélectionnez l'interface.

Étape 8 Pour les filtres sortants, vous pouvez éventuellement spécifier le protocole, pour limiter le filtre aux routes annoncées à ce processus de routage.

Il existe deux formes de la commande **distribute-list out**, une avec une variable *d'identifiant* après la variable *de protocole* et l'autre sans l'identifiant. Vous pouvez sélectionner les protocoles suivants, mais ils sont répartis entre ces versions de commande selon que vous devez fournir les informations d'identifiant supplémentaires.

- **connected**. Pour les routes établies pour les réseaux qui sont directement connectés aux interfaces du système.
- **static**. Pour les routes statiques que vous avez créées manuellement.
- **rip**. Pour les routes annoncées à RIP.
- **bgp** *système autonome*. Pour les routes annoncées à BGP. Cliquez sur *l'identifiant* et saisissez le numéro de système autonome pour le processus BGP défini sur le système.
- **eigrp** *système autonome*. Pour les routes annoncées à l'EIGRP. Cliquez sur *l'identifiant* et saisissez le numéro de système autonome pour le processus EIGRP défini sur le système.

- **ospf** *process-id*. Pour les routes annoncées à OSPF. Cliquez sur *l'identifiant* et saisissez l'ID de processus pour l'autre processus OSPF défini sur le système.

Étape 9 Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **configure filter-rules** pour définir une autre règle de filtre. Définissez-en autant que vous le souhaitez.

Étape 10 Cliquez sur **OK**.

Configurer la redistribution OSPF

Vous pouvez contrôler la redistribution des routes dans un processus OSPF à partir d'autres protocoles de routage, des routes connectées et des routes statiques.

Avant de commencer

Il est conseillé de configurer le processus de routage à partir duquel vous redistribuerez les routes et de déployer vos modifications avant de configurer la redistribution dans OSPF.

Si vous souhaitez appliquer une carte de routage pour affiner les routes redistribuées, créez l'objet de carte de routage Smart CLI. Les routes qui correspondent à la carte de routage sont redistribuées, et toutes les routes qui ne correspondent pas ne sont pas redistribuées.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez OSPF.

Étape 3 Cliquez sur l'onglet **OSPF**.

Étape 4 Ajoutez ou modifiez un objet de processus OSPF.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) pour exposer toutes les commandes, puis cliquez sur **+** pour activer la commande **configure redistribution**.

Étape 6 Cliquez sur la variable *protocol* (protocole) et sélectionnez le processus source à partir duquel vous redistribuez les routes. Vous pouvez redistribuer les routes **connected** et **static**, ou les routes générées par **bgp**, **eigrp**, **isis**, **ospf**, ou **rip**.

Étape 7 Si vous sélectionnez un processus de routage, cliquez sur la variable *identifier* (identifiant) et saisissez la valeur requise :

- **bgp**, **eigrp**. Saisissez le numéro du système autonome.
- **ospf**. Saisissez le numéro d'ID de processus.
- **connected**, **static**, **isis**, **rip**. Entrez **none**. Même si vous saisissez une valeur différente, elle sera ignorée.

Étape 8 (Facultatif ; IS-IS uniquement.) Dans la commande **redistribute isis level-2**, cliquez sur **level-2** et sélectionnez si vous redistribuez les routes apprises uniquement dans une zone IS-IS (**level-1**), entre les zones IS-IS (**level-2**) ou les deux (**level-1-2**).

Étape 9 (Facultatif ; tous les protocoles.) Si vous appliquez des balises aux routes afin de contrôler la redistribution, cliquez sur **+** pour activer la commande **redistribute tag** *numéro de balise*, puis cliquez sur la variable et saisissez la balise associée aux routes que vous souhaitez redistribuer. Le numéro de balise est compris entre 0 et 4294967295.

Étape 10 (Facultatif ; tous les protocoles.) Si vous souhaitez redistribuer les routes pour tous les sous-réseaux, pas seulement ceux qui respectent la classe standard, cliquez sur **+** pour activer la commande **redistribute subnets**.

Par exemple, si vous n'activez pas cette commande, une route spécifique pour 10.100.10.0/24 ne sera pas redistribuée; au lieu de cela, seule une route pour 10.0.0.0/8 serait redistribuée.

Étape 11 (Facultatif ; tous les protocoles.) Pour affiner les routes redistribuées en fonction d'une carte de routage, cliquez sur le signe **plus (+)** pour activer la commande **redistribute** *carte de routage*, cliquez sur la variable et sélectionnez la carte de routage qui définit vos restrictions.

Si vous n'appliquez pas de carte de routage, toutes les routes du processus (qui correspondent aux autres commandes configurées pour la redistribution) sont redistribuées.

Étape 12 (Facultatif ; tous les protocoles.) Pour affiner les mesures pour les routes redistribuées, cliquez sur **+** pour activer la commande suivante et configurer les options :

redistribute *protocol* **metric** *metric-value* **metric-type** *metric-type-value*

Cliquez sur les variables pour configurer les éléments suivants :

- **metric**. La valeur de mesure pour les routes en cours de distribution, de 0 à 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.
- **metric-type**. 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 OSPF. Les options disponibles sont 1 pour un routage externe de type 1 ou 2 pour un routage externe de type 2. La valeur par défaut est 2.

Étape 13 (Facultatif ; OSPF uniquement.) Les commandes suivantes sont activées par défaut lorsque vous redistribuez les routes d'un autre processus OSPF. Vous pouvez cliquer sur **-** pour désactiver les commandes indésirables.

Ces commandes précisent les critères selon lesquels les routes OSPF sont redistribuées dans d'autres domaines de routage.

- **redistribute ospf match external 1**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 1.
- **redistribute ospf match external 2**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 2.
- **redistribute ospf match internal**. Routes internes à un système autonome spécifique.
- **redistribute ospf match nssa-external 1**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 1 et marquées comme Not-So-Stubby-Area (NSSA) uniquement.
- **redistribute ospf match nssa-external 2**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 2 et marquées comme Not-So-Stubby-Area (NSSA) uniquement.

Étape 14 Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **configure redistribution** pour configurer la redistribution pour un autre protocole. Configurez la redistribution pour chaque protocole qui a du sens pour votre réseau.

Étape 15 Cliquez sur **OK**.

Configurer les paramètres de l'interface OSPFv2 et l'authentification OSPF

Toute interface qui fait face à un routeur OSPF voisin communique avec ce dernier à l'aide de paquets Hello et d'autres méthodes pour vérifier l'intégrité du voisin et pour partager les mises à jour de routage. Bien que certaines de ces caractéristiques aient des paramètres par défaut, il est conseillé de définir les options explicitement à l'aide d'un objet de paramètres d'interface OSPF. Créez un objet pour chaque interface adjacente à un routeur voisin OSPF.

Remarque Les routeurs d'un réseau donné doivent avoir les mêmes valeurs pour l'authentification et pour les intervalles Hello et morts de détection de voisin perdu.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez OSPF.

Étape 3 Cliquez sur l'onglet **OSPF**.

Étape 4 Effectuez l'une des opérations suivantes :

- Pour créer un nouvel objet, cliquez sur **+** > **OSPF Interface Settings (Paramètres d'interface OSPF)** ou cliquez sur le bouton **Create OSPF Object (Créer un objet OSPF)** > **OSPF Interface Settings (Paramètres d'interface OSPF)**.
- Cliquez sur l'icône de modification ( ) de l'objet que vous souhaitez modifier. Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Si vous n'avez plus besoin d'un objet de paramètres d'interface, cliquez sur l'icône de la corbeille pour supprimer l'objet.

Étape 5 Entrez un nom pour l'objet et, facultativement, une description.

Étape 6 Configurez l'authentification pour l'interface.

configure authentication *auth-type*

Pour configurer l'authentification OSPF, vous devez configurer le mot de passe ou la clé d'authentification sur chacune des interfaces OSPF, puis activer l'authentification sur la zone elle-même. Vous devez choisir la même méthode d'authentification sur les interfaces et la zone.

Vous pouvez sélectionner les options suivantes en cliquant sur *auth-type*.

- **none** : n'utilisez pas l'authentification OSPF. Tout routeur OSPF fonctionnant sur la liaison peut établir une contiguïté avec ce routeur. La commande suivante est ajoutée à l'objet : **ospf authentication null**.
- **password** : authentifier la connexion OSPF à l'aide d'un mot de passe partagé. Vous pouvez configurer un mot de passe distinct pour chaque réseau interface par interface. Cependant, tous les routeurs voisins sur le même réseau doivent avoir le même mot de passe pour pouvoir échanger des informations OSPF.

  Lorsque vous sélectionnez cette option, deux commandes sont ajoutées : **ospf authentication** et **ospf authentication-key** *key*. Cliquez sur la variable pour configurer les éléments suivants :

  - *key* : sélectionnez l'objet de clé secrète qui contient le mot de passe. Le mot de passe peut comporter jusqu'à 8 caractères. Vous pouvez inclure un espace vide entre deux caractères. Les espaces au début ou à la fin du mot de passe sont ignorés. Si l'objet n'existe pas encore, cliquez sur **Create New Secret Key** (Créer une nouvelle clé secrète) en bas de la liste et créez-la maintenant.

- **message-digest** : authentifier la connexion OSPF à l'aide du condensé du message (MD5). L'authentification MD5 vérifie l'intégrité de la communication, authentifie l'origine et vérifie l'exactitude de la communication. Les deux routeurs doivent être configurés pour utiliser la même clé MD5.

  Lorsque vous sélectionnez cette option, deux commandes sont ajoutées : **ospf authentication message-digest** et **ospf message-digest-key** *key-id* **md5** *key*. Cliquez sur les variables pour configurer les éléments suivants :

  - *key-id* : numéro d'ID de la clé d'authentification, de 1 à 255. Vous devez configurer le routeur voisin avec le même ID de clé et la clé MD5 associée.
  - *key* (clé) : sélectionnez l'objet de clé secrète qui contient la clé MD5. Le mot de passe peut comporter jusqu'à 16 caractères alphanumériques. Vous pouvez inclure des espaces entre les caractères. Les espaces au début ou à la fin de la clé sont ignorés. Si l'objet n'existe pas encore, cliquez sur **Create New Secret Key** (Créer une nouvelle clé secrète) en bas de la liste et créez-la maintenant.

Étape 7 (Facultatif) Configurez les minuteries d'annonce d'état de liaison (LSA).

Ces minuteurs ont des valeurs par défaut, vous ne devez donc les modifier que si votre réseau nécessite des paramètres différents. Configurez les commandes suivantes :

- **ospf retransmit interval 5** : le nombre de secondes entre les retransmissions de LSA pour les contiguïtés appartenant à une interface OSPF. La durée doit être supérieure au délai aller-retour attendu entre deux routeurs du réseau connecté. La plage est comprise entre 1 et 8 192 secondes. La valeur par défaut est de 5 secondes. Cliquez sur le 5 et saisissez un nouveau nombre pour modifier la valeur.
- **ospf transmit-delay 1** : estimation du nombre de secondes nécessaires pour envoyer un paquet de mise à jour d'état de liaison sur une interface OSPF, de 1 à 8 192 secondes. La valeur par défaut est de 1 seconde. Cliquez sur le 1 et saisissez un nouveau nombre pour modifier la valeur.

Étape 8 (Facultatif) Tous les autres paramètres ont des valeurs par défaut ou sont facultatifs. Modifiez-les ou activez-les uniquement si vous avez besoin d'un comportement différent. Cliquez sur le lien **Show Disabled** (Afficher les éléments désactivés) pour afficher les options.

Voici les paramètres d'interface supplémentaires. Pour activer un paramètre, cliquez sur le **+** à gauche de la commande, puis configurez la commande (si nécessaire).

- **ospf cost** *valeur* : le coût (une mesure d'état de liaison) de l'envoi d'un paquet sur une interface OSPF, de 1 à 65 535. La valeur 1 représente un réseau directement connecté à l'interface. Cliquez sur la variable

et saisissez le coût qui représente la capacité de l'interface en fonction des chiffres que vous utilisez dans votre réseau.

Au moment de décider d'une valeur, plus la bande passante de l'interface est élevée, plus le coût associé pour l'envoi des paquets sur cette interface doit être faible. En d'autres termes, une valeur de coût élevée représente une interface à faible bande passante et une valeur de coût faible représente une interface à bande passante élevée. Le numéro spécifique que vous sélectionnez n'a aucune signification inhérente : la valeur est relative aux autres valeurs que vous configurez pour l'interface dans la zone OSPF. Ces valeurs affectent ensuite le calcul de la meilleure route pour une destination.

Le coût par défaut de l'interface OSPF sur le périphérique Firepower Threat Defense est de 10. Ce coût par défaut diffère du logiciel Cisco IOS, où le coût par défaut est de 1 pour Fast Ethernet et Gigabit Ethernet et de 10 pour 10BaseT. Il est important d'en tenir compte si vous utilisez ECMP dans votre réseau.

- **ospf database-filter all out** : filtre tous les LSA sortants vers une interface OSPF lors de la synchronisation et de l'injection.
- **ospf mtu-ignore** : désactive la détection de non-concordance d'unité de transmission maximale (MTU) OSPF lors de la réception des paquets de base de données. 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 configurée sur l'interface entrante, la contiguïté OSPF n'est pas établie. Si vous ne pouvez pas corriger les valeurs MTU sur les interfaces, vous pouvez désactiver la vérification MTU.
- **ospf network point-to-point non-broadcast** : configure l'interface OSPF comme un réseau point à point, sans diffusion. Cela vous permet de transmettre des routes OSPF sur des tunnels VPN. Si vous configurez cette option, la découverte dynamique des voisins n'est pas possible. Vous devez également :
  - Mettre à jour l'objet de processus OSPF pour définir un seul voisin statique pour cette interface. Mettre également à jour le processus OSPF du routeur voisin pour définir ce périphérique comme son voisin statique.
  - Créer des routes statiques (sur chaque routeur) qui pointent vers le routeur voisin.
- **ospf priority** *valeur* : la priorité du routeur par rapport aux autres routeurs du réseau, de 0 à 255. La priorité par défaut est 1. Lorsque deux routeurs connectés à un réseau tentent tous deux de devenir le routeur désigné, le routeur ayant la priorité de routeur la plus élevée prévaut. En cas d'égalité, le routeur ayant l'ID de routeur le plus élevé devient le routeur désigné. Un routeur dont la priorité de routeur est définie à zéro ne peut pas devenir le routeur désigné ou le routeur désigné de secours. Cliquez sur la variable et sélectionnez la priorité en fonction du système de numérotation relative que vous utilisez dans votre réseau.
- **ospf lost-neighbor-detection** *mécanisme de détection* : définit comment le système détermine si un routeur voisin est en panne. OSPF doit recréer les routes chaque fois qu'un routeur OSPF est déclaré en panne. Pour des informations détaillées sur la configuration de la détection des voisins perdus, consultez Configurer la détection de voisin perdu OSPFv2 et les paquets Fast Hello (paramètres de l'interface OSPF), à la page 398.

Étape 9 Cliquez sur **OK**.

Configurer la détection de voisin perdu OSPFv2 et les paquets Fast Hello (paramètres de l'interface OSPF)

Le processus OSPF envoie régulièrement des paquets Hello à chaque routeur voisin pour vérifier que le voisin peut toujours répondre. L'échec continu de la réponse indique que le routeur voisin (entièrement ou seulement l'interface adjacente) n'est pas disponible pour le routage, et OSPF doit recalculer les routes et le système OSPF doit converger sur la table de routage mise à jour.

Vous pouvez ajuster les valeurs suivantes pour affiner votre réseau. Idéalement, vous souhaitez réduire au minimum la fréquence de déclaration des voisins vers le bas et le calcul des routes. D'un autre côté, vous souhaitez également minimiser le temps nécessaire au réseau pour reconverger sur une bonne table de routage lorsqu'un routeur (ou une interface) OSPF est vraiment en panne.

- Intervalle Hello : il s'agit du délai entre l'envoi de paquets Hello. La valeur par défaut est de 10 secondes. Si vous le souhaitez, vous pouvez configurer des paquets Hello rapides, où les hellos sont envoyés à des intervalles de sous-seconde. Les paquets Hello rapides permettent la détection plus rapide d'un voisin en panne et la reconvergence de la table de routage.
- Intervalle mort : la durée pendant laquelle, si aucun paquet Hello n'est vu d'un voisin, le voisin est déclaré mort. La valeur par défaut est de 40 secondes (4 fois l'intervalle Hello par défaut), sauf si vous utilisez des paquets Hello rapides, auquel cas l'intervalle mort est toujours de 1 seconde. La définition d'un intervalle mort plus petit permettra une détection plus rapide d'un voisin en panne et améliorera la convergence, mais pourrait entraîner une plus grande instabilité de routage. Dans tous les cas, vous devez configurer l'intervalle mort pour qu'il soit supérieur à l'intervalle Hello. Vous devez définir le même intervalle mort sur tous les routeurs OSPF du réseau.

Vous configurez la détection du voisin perdu dans l'objet des paramètres de l'interface OSPF.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez OSPF.

Étape 3 Cliquez sur l'onglet **OSPF**.

Étape 4 Effectuez l'une des opérations suivantes :

- Pour créer un nouvel objet, cliquez sur **+** > **OSPF Interface Settings (Paramètres d'interface OSPF)** ou cliquez sur le bouton **Create OSPF Object (Créer un objet OSPF)** > **OSPF Interface Settings (Paramètres d'interface OSPF)**.
- Cliquez sur l'icône de modification ( ) de l'objet que vous souhaitez modifier. Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Étape 5 Si la commande **ospf lost-neighbor-detection** *detection-mechanism* ne s'affiche pas, cliquez sur le lien **Show Disabled** (Afficher les éléments désactivés).

Étape 6 Cliquez sur le **+** à gauche de la commande pour l'activer.

Étape 7 Cliquez sur *detection-mechanism* et sélectionnez le mécanisme que vous souhaitez mettre en œuvre :

- **dead-interval** : pour configurer un intervalle Hello standard en secondes. Les commandes suivantes sont ajoutées ; ajustez leurs valeurs au besoin :
  - **ospf hello-interval 10** : intervalle Hello, de 1 à 8 192 secondes. La valeur par défaut est 10. Cette valeur doit être inférieure à l'intervalle mort. Cliquez sur la valeur pour saisir le nombre souhaité.
  - **ospf dead-interval 40** : intervalle mort, de 1 à 8 192 secondes. La valeur conseillée est de 4 fois l'intervalle Hello, mais vous pouvez configurer un délai plus court pour une convergence plus rapide.
- **hello-multiplier** : pour configurer des paquets Fast Hello à la sous-seconde. La commande suivante est ajoutée, vous devez configurer la valeur.
  - **ospf dead-interval minimal hello-multiplier** *value* : cliquez sur la variable et saisissez le nombre de paquets Hello qui doivent être envoyés chaque seconde, de 3 à 20. L'intervalle mort est défini à 1 seconde par le mot-clé **minimal**.

Étape 8 Cliquez sur **OK**.

Supervision OSPF

Pour surveiller et dépanner OSPF, ouvrez la console de l'interface de ligne de commande ou connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes. Vous pouvez également sélectionner certaines de ces commandes dans le menu **Commands (Commandes)** sur la page Routing (Routage).

Utilisez **show ospf ?** pour obtenir des listes d'options supplémentaires. Par exemple, vous pouvez spécifier l'ID de processus, l'ID de zone et le routeur virtuel pour limiter les informations que vous voyez, ainsi que d'autres options pour cibler uniquement les informations que vous recherchez. La liste suivante n'est qu'un résumé.

- **show ospf**

  Affiche des informations générales sur les processus de routage OSPFv2.

- **show ospf border-routers**

  Affiche les entrées de la table de routage OSPFv2 interne pour l'ABR et l'ASBR.

- **show ospf database**

  Affiche les listes d'informations liées à la base de données OSPFv2 pour un routeur spécifique.

- **show ospf events**

  Affiche les informations sur les événements internes d'OSPF.

- **show ospf flood-list**

  Affiche une liste des LSA en attente d'être diffusés sur une interface, pour observer la cadence des paquets OSPFv2. Les paquets de mise à jour OSPFv2 sont automatiquement cadencés afin qu'ils ne soient pas envoyés à moins de 33 millisecondes d'intervalle. Sans cadence, certains paquets de mise à jour pourraient se perdre dans des situations où la liaison est lente, un voisin ne pourrait pas recevoir les mises à jour assez rapidement ou le routeur pourrait manquer d'espace tampon.

La cadence est également utilisée entre les renvois pour accroître l'efficacité et réduire au minimum les retransmissions perdues. Vous pouvez également afficher les LSA en attente d'envoi depuis une interface. La cadence permet d'envoyer plus efficacement les paquets de mise à jour et de retransmission OSPFv2.

- **show ospf interface**

  Affiche les informations de l'interface liées à OSPFv2.

- **show ospf neighbor**

  Affiche les informations sur les voisins OSPFv2 pour chaque interface.

- **show ospf nsf**

  Affiche les informations de transfert sans arrêt (NSF) liées à OSPFv2.

- **show ospf request-list**

  Affiche une liste de tous les LSA demandés par un routeur.

- **show ospf retransmission-list**

  Affiche une liste de tous les LSA en attente de renvoi.

- **show ospf rib**

  Affiche la base d'informations du routeur OSPF (RIB).

- **show ospf statistics**

  Affiche diverses statistiques OSPF, notamment le nombre d'exécutions du SPF, les raisons et la durée.

- **show ospf summary-addresses**

  Affiche la liste de toutes les informations de redistribution d'adresses sommaires configurées dans un processus OSPFv2.

- **show ospf traffic**

  Affiche une liste des différents types de paquets envoyés ou reçus par une instance OSPFv2 spécifique.

- **show ospf virtual-links**

  Affiche les informations sur les liens virtuels liés à OSPFv2.



CHAPITRE 16

Protocole de routage de passerelle intérieure amélioré (EIGRP)

Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) est un protocole de routage de passerelle intérieure hybride à vecteur de distance dynamique et à état de liaison. À l'origine un protocole propriétaire mis au point par Cisco, il s'agit maintenant d'une norme ouverte définie dans la RFC 7868. Vous pouvez configurer le protocole EIGRP pour gérer les routes intérieures dans un système autonome.

- Bonnes pratiques pour l'EIGRP, à la page 401
- À propos d'EIGRP, à la page 402
- Lignes directrices relatives à l'EIGRP, à la page 403
- Configurer le processus Core EIGRP, à la page 404
- Personnaliser le processus EIGRP, à la page 408
- Surveillance EIGRP, à la page 418

Bonnes pratiques pour l'EIGRP

Voici quelques conseils pour la configuration d'EIGRP :

- Si vous insérez le périphérique dans un système autonome EIGRP existant, examinez la configuration des autres routeurs dans le système autonome pour déterminer le numéro de système et toute autre personnalisation. Assurez-vous de mettre en œuvre les mêmes personnalisations, ou du moins des personnalisations constantes, sur le périphérique Firewall Threat Defense que vous ajoutez.
- Déterminez s'il faut configurer un processus EIGRP complet ou un processus de talon :
  - Si le périphérique Firewall Threat Defense se trouve au milieu du système autonome, où il est connecté à plusieurs autres routeurs EIGRP, vous avez probablement besoin du processus EIGRP complet. Consultez Configurer le processus EIGRP pour le routage complet, à la page 404.
  - Si le périphérique Firewall Threat Defense se trouve à la périphérie du système autonome, où il est connecté à un seul autre routeur EIGRP et où il héberge uniquement les réseaux connectés, sa configuration en tant que routeur de talon peut être plus logique. Vous pouvez configurer le talon de sorte que le périphérique Firewall Threat Defense envoie des informations au voisin d'EIGRP au sujet des routes connectées, afin que d'autres routeurs EIGRP dans le système autonome puissent obtenir des routes vers les réseaux connectés du périphérique Firewall Threat Defense. Consultez Configurer le processus EIGRP pour le routage de talon, à la page 405.

- Les paramètres par défaut fonctionnent pour la plupart des réseaux. Ne les ajustez donc que si vous les avez ajustés sur d'autres routeurs EIGRP dans le système autonome. Vous pouvez avoir un processus EIGRP entièrement fonctionnel en configurant simplement le numéro de système autonome et en précisant les réseaux à acheminer.
- Configurez l'ID de routeur pour vous assurer qu'une adresse stable est utilisée pour identifier le routeur. Cela peut faciliter la résolution des problèmes de routage. Consultez Configurer les paramètres avancés EIGRP, à la page 408.
- N'activez pas la récapitulation automatique du routage (la commande **auto-summary**), sauf si vous avez déterminé qu'elle ne créera pas de boucles de routage et qu'elle procurera un certain avantage à votre réseau. La façon de déterminer si la récapitulation automatique fonctionnera pour votre réseau n'entre pas dans le cadre de ce document.

À propos d'EIGRP

Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) est un protocole de routage de passerelle intérieure hybride à vecteur de distance dynamique et à état de liaison. EIGRP envoie des mises à jour de routage aux routeurs du même système autonome. Normalement, EIGRP découvre les routeurs voisins à l'aide de mises à jour de multidiffusion, mais vous pouvez configurer des voisins statiques situés hors de la zone de multidiffusion ; ces voisins recevront alors des mises à jour unicast.

La technologie de convergence de l'EIGRP repose sur un algorithme appelé Diffusing Update Algorithm (DUAL). L'algorithme garantit un fonctionnement sans boucle à tout moment durant le calcul du routage, et permet à tous les périphériques impactés par un changement de topologie de se synchroniser. Les périphériques non touchés par le changement de topologie ne sont pas concernés par les recalculs.

Vous pouvez, dans une certaine mesure, ajuster les métriques de routage pour contrôler la sélection des routes. Les rubriques suivantes fournissent des informations de base sur ces concepts avancés.

Remarque Si vous ajustez ces métriques, vous devez appliquer les mêmes ajustements à tous les routeurs du système autonome, faute de quoi vous risquez de provoquer des boucles de routage.

Machine à états finis DUAL

La machine à états finis DUAL matérialise le processus de décision pour tous les calculs de routage. Elle suit toutes les routes annoncées par tous les voisins. DUAL utilise les informations de distance (connues sous le nom de métrique) pour sélectionner des chemins efficaces et sans boucle.

DUAL sélectionne les routes à insérer dans une table de routage en fonction des successeurs possibles. Un successeur est un périphérique voisin, utilisé pour le transfert de paquets, qui a un chemin de moindre coût vers une destination et garantit l'absence de boucle de routage.

Lorsqu'un changement de topologie se produit, DUAL teste pour rechercher des successeurs possibles. S'il existe des successeurs possibles, DUAL utilisera tous les successeurs possibles qu'il trouve pour éviter une recomputation inutile.

Lorsqu'il n'y a pas de successeurs possibles, mais que seuls les voisins communiquent la destination, un nouveau calcul doit avoir lieu pour déterminer un nouveau successeur. Le temps nécessaire pour recomputer la route affecte le temps de convergence.

Poids métriques EIGRP

L'EIGRP utilise des poids métriques, appelés valeurs K, dans les calculs de routage et de métriques. Les valeurs par défaut des mesures EIGRP ont été sélectionnées avec soin pour fournir des performances optimales dans la plupart des réseaux.

Contrairement aux routeurs IOS, vous ne pouvez pas ajuster ces valeurs K par défaut pour l'EIGRP exécuté sur le périphérique Firewall Threat Defense. Comme vous devez utiliser les mêmes valeurs K sur tous les systèmes d'un réseau autonome, vous ne devez pas les modifier sur les routeurs d'un système autonome qui comprend des périphériques Firewall Threat Defense.

Pour obtenir une explication de l'utilisation des valeurs K, consultez Mesures de coût EIGRP, à la page 403.

Mesures de coût EIGRP

EIGRP utilise des pondérations de mesure (valeurs K) en plus des caractéristiques de liaison pour calculer une mesure de coût composée. Pour éviter la perturbation du réseau à la suite d'une modification des caractéristiques de la liaison, vous pouvez régler certaines des valeurs utilisées dans ce calcul.

Le calcul réel est assez complexe, utilisant cinq valeurs K (comme multiplicateurs) et cinq attributs de vecteur. Cependant, trois valeurs K sont 0 par défaut et, comme vous ne pouvez pas modifier la valeur K par défaut, le calcul réel est vraiment simplifié :

mesure de coût = 256 × (bande passante + retard)

Ce que vous pouvez modifier, ce sont les valeurs de bande passante et de délai pour les routes redistribuées à partir du processus EIGRP. Plus précisément, vous pouvez ajuster ces valeurs dans la commande **default-metric** (pour définir une valeur par défaut pour tous les types de routes redistribuées) ou dans la commande **redistribute metric** (pour définir les mesures pour un type de route spécifique). Tenez compte des points suivants :

- Bande passante : la bande passante minimale de la voie de routage en kilobits par seconde. Elle peut être comprise entre 1 et 4 294 967 295 kilobits par seconde. La bande passante pour la formule est mise à l'échelle et inversée par la formule suivante :

  $(10^7$/bande passante minimale en kilobits par seconde)

- Retard : le retard de routage en dizaines de microsecondes.

Les autres caractéristiques, qui ne sont pas utilisées par Firewall Threat Defense, sont la confiance dans le délai, la charge effective sur la route et la MTU minimale (unité maximale de transmission) sur la route. Même si les valeurs ne sont pas utilisées, vous devez les configurer si vous ajustez ces commandes.

Pour des informations plus détaillées sur la façon dont EIGRP calcule la mesure de coût, consultez *Routage IP : Guide de configuration EIGRP*. Par exemple, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16-7/ire-xe-16-8-book/ire-enhanced-igrp.html.

Lignes directrices relatives à l'EIGRP

Directives IPv6

Ne prend pas en charge IPv6.

Directives supplémentaires

- Un maximum d'un processus EIGRP est pris en charge.
- Vous ne pouvez pas modifier le numéro de système autonome d'un processus EIGRP. Supprimez plutôt le processus, déployez vos modifications, puis configurez un nouveau processus avec le nouveau numéro de système autonome.
- Vous ne pouvez pas inclure un réseau dans le processus EIGRP qui appartient à une interface virtuelle de pont (BVI).
- 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.

Configurer le processus Core EIGRP

Les rubriques suivantes expliquent comment configurer et exécuter l'EIGRP sur le périphérique. Vous pouvez soit configurer le processus de routage complet, soit le configurer en tant que processus de talon pour les systèmes qui ne doivent pas participer entièrement au réseau autonome en tant que routeur EIGRP.

Configurer le processus EIGRP pour le routage complet

Vous pouvez configurer un processus EIGRP au maximum. Si vous configurez plusieurs routeurs virtuels, EIGRP est pris en charge dans le routeur virtuel global uniquement.

La procédure suivante configure le routage EIGRP de base pour un ensemble de réseaux en utilisant toutes les valeurs par défaut pour le routage EIGRP. L'exécution de cette procédure est suffisante pour activer l'EIGRP sur le périphérique. Vous pouvez effectuer les autres procédures pour affiner le processus EIGRP au besoin.

Avant de commencer

Déterminez le numéro de système autonome que vous utilisez pour l'EIGRP dans votre réseau.

Créez des objets réseau qui définissent chacun des réseaux que vous souhaitez acheminer dans le système autonome EIGRP. Par exemple, si vous souhaitez utiliser EIGRP pour les réseaux 192.168.1.0/24 et 192.168.2.0/24, créez deux objets réseau, un pour chaque réseau.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) du routeur virtuel global.

Étape 3 Cliquez sur l'onglet **EIGRP**.

Étape 4 Effectuez l'une des opérations suivantes :

- Pour créer un nouveau processus, cliquez sur **+** ou sur le bouton **Create EIGRP Object** (Créer un objet EIGRP).
- Cliquez sur l'icône de modification () de l'objet que vous souhaitez modifier. Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Si vous n'avez plus besoin d'un processus, cliquez sur l'icône de la corbeille pour supprimer l'objet.

Étape 5 Saisissez un **Name (Nom)** pour l'objet Smart CLI et, au besoin, une description.

Étape 6 Configurez les propriétés de base du processus :

router eigrp *autonomous-system (système autonome)*

Cliquez sur la variable et saisissez un nombre compris entre 1 et 65 535. Utilisez le même numéro de système autonome utilisé sur les autres routeurs du réseau qui doit fonctionner dans le même domaine de routage que ce périphérique.

Étape 7 Configurez les réseaux et les interfaces qui doivent être routées dans le système autonome EIGRP.

a) Cliquez sur le lien **Show Disabled** (Afficher les éléments désactivés) au-dessus du corps de l'objet pour ajouter toutes les autres lignes de configuration possibles.

b) Cliquez sur le **+** à gauche de la ligne **network** *network-object*.

c) Dans la commande **network**, cliquez sur la variable et sélectionnez l'objet qui définit un réseau qui doit être inclus dans ce système autonome.

En règle générale, il s'agirait d'un réseau directement connecté. Par exemple, si l'adresse IP de l'interface interne est 192.168.1.1/24, l'objet réseau associé à cette commande contiendra 192.168.1.0/24. Si l'objet n'existe pas encore, cliquez sur **Create New Network** (Créer un nouveau réseau) pour le créer maintenant.

Les réseaux directement connectés et statiques qui appartiennent au réseau défini sont annoncés par le processus. De plus, seules les interfaces ayant une adresse IP qui entre dans le réseau défini participent au processus de routage EIGRP.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, consultez Configurer les interfaces de routage passif EIGRP, à la page 411.

d) Si vous avez d'autres réseaux à acheminer, cliquez sur **…** > **Duplicate** > **(Dupliquer)** à gauche de la commande **network** pour en ajouter une nouvelle. Continuez à ajouter des lignes **network** jusqu'à ce que vous ayez configuré tous les réseaux pour le routage.

Étape 8 (Facultatif) Si nécessaire, ajustez les paramètres des autres commandes initialement désactivées. Consultez Personnaliser le processus EIGRP, à la page 408

Étape 9 Cliquez sur **OK**.

Configurer le processus EIGRP pour le routage de talon

Vous pouvez configurer le périphérique pour qu'il soit un routeur de talon EIGRP. Le routage de talon réduit les exigences de mémoire et de traitement sur le système. En tant que routeur de talon, le système 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 de talon, le système répond à toutes les requêtes de résumés, de routes connectées, de routes statiques redistribuées, de routes externes et de routes internes avec le message « inaccessible ». Le système envoie un paquet d'informations d'homologue spécial à tous les routeurs voisins pour signaler son état de routeur de talon. 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.

Avant de commencer

Déterminez le numéro de système autonome que vous utilisez pour l'EIGRP dans votre réseau.

Créez des objets réseau qui définissent chacun des réseaux que vous souhaitez acheminer dans le système autonome EIGRP. Par exemple, si vous souhaitez utiliser EIGRP pour les réseaux 192.168.1.0/24 et 192.168.2.0/24, créez deux objets réseau, un pour chaque réseau.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) du routeur virtuel global.

Étape 3 Cliquez sur l'onglet **EIGRP**.

Étape 4 Effectuez l'une des opérations suivantes :

- Pour créer un nouveau processus, cliquez sur **+** ou sur le bouton **Create EIGRP Object** (Créer un objet EIGRP).
- Cliquez sur l'icône de modification ( ) de l'objet que vous souhaitez modifier. Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Si vous n'avez plus besoin d'un processus, cliquez sur l'icône de la corbeille pour supprimer l'objet.

Étape 5 Saisissez un **Name (Nom)** pour l'objet Smart CLI et, au besoin, une description.

Étape 6 Configurez les propriétés de base du processus :

router eigrp *autonomous-system (système autonome)*

Cliquez sur la variable et saisissez un nombre compris entre 1 et 65 535. Utilisez le même numéro de système autonome utilisé sur les autres routeurs du réseau qui doit fonctionner dans le même domaine de routage que ce périphérique.

Étape 7 Configurez les réseaux et les interfaces qui doivent être routées dans le système autonome EIGRP.

a) Cliquez sur le lien **Show Disabled** (Afficher les éléments désactivés) au-dessus du corps de l'objet pour ajouter toutes les autres lignes de configuration possibles.

b) Cliquez sur le **+** à gauche de la ligne **network** *network-object*.

c) Dans la commande **network**, cliquez sur la variable et sélectionnez l'objet qui définit un réseau qui doit être inclus dans ce système autonome.

En règle générale, il s'agirait d'un réseau directement connecté. Par exemple, si l'adresse IP de l'interface interne est 192.168.1.1/24, l'objet réseau associé à cette commande contiendra 192.168.1.0/24. Si l'objet n'existe pas encore, cliquez sur **Create New Network** (Créer un nouveau réseau) pour le créer maintenant.

Les réseaux directement connectés et statiques qui appartiennent au réseau défini sont annoncés par le processus. De plus, seules les interfaces ayant une adresse IP qui entre dans le réseau défini participent au processus de routage EIGRP.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, consultez Configurer les interfaces de routage passif EIGRP, à la page 411.

d) Si vous avez d'autres réseaux à acheminer, cliquez sur **…** > **Duplicate** > **(Dupliquer)** à gauche de la commande **network** pour en ajouter une nouvelle. Continuez à ajouter des lignes **network** jusqu'à ce que vous ayez configuré tous les réseaux pour le routage.

Étape 8 Configurez les paramètres du talon.

a) Cliquez sur le **+** à gauche de la ligne **setup eigrp** *de configuration*.

b) Cliquez sur la variable et sélectionnez **advanced**.

c) Cliquez sur le **+** à gauche de la commande **setup eigrp stub** *stub-options*.

d) Pour empêcher le périphérique de partager l'une de ses routes avec tout autre routeur du système autonome, afin qu'il ne reçoive que les mises à jour du routeur voisin EIGRP, cliquez sur *stub-options* et sélectionnez **receive**. Configurez ensuite la commande suivante :

eigrp stub *stub-parameters*

Cliquez sur la variable et sélectionnez **receive-only**.

e) Pour permettre au périphérique d'annoncer les routes aux routeurs voisins EIGRP, cliquez sur *stub-options* et sélectionnez **other**. Configurez ensuite la commande suivante pour sélectionner les types de routage qui doivent être annoncés.

eigrp stub *connected-parameter redistributed-parameter static-parameter summary-parameter*

Cliquez sur les variables pour effectuer votre sélection. Vous devez sélectionner au moins un type de routage, mais vous pouvez sélectionner tous les types de routage ou n'importe quelle combinaison.

- *connected-parameter*. Sélectionnez **connected** pour annoncer les routes connectées. Si les routes connectées ne sont pas couvertes par une instruction **network**, il sera peut-être nécessaire de configurer la redistribution pour les routes connectées dans le processus EIGRP.
- *redistributed-parameter*. Sélectionnez **redistributed** pour annoncer les routes redistribuées dans le processus de routage EIGRP à partir d'autres protocoles de routage.
- *static-parameter*. Sélectionnez **static** pour annoncer les routes statiques. Vous devez également activer la commande **configure redistribution** et configurer la redistribution des routes statiques.
- *summary-parameter*. Sélectionnez **summary** pour annoncer les routes récapitulatives.

Étape 9 (Facultatif) Si nécessaire, ajustez les paramètres des autres commandes initialement désactivées. Consultez Personnaliser le processus EIGRP, à la page 408

Étape 10 Cliquez sur **OK**.

Personnaliser le processus EIGRP

EIGRP comprend de nombreuses options qui ont des valeurs par défaut. Ces valeurs fonctionnent bien pour de nombreux réseaux. Cependant, vous devrez peut-être ajuster un ou plusieurs paramètres pour obtenir le comportement précis dont vous avez besoin. Les rubriques suivantes expliquent les différentes façons de personnaliser votre processus de routage EIGRP.

Configurer les paramètres avancés EIGRP

Vous pouvez configurer plusieurs paramètres qui contrôlent le comportement global d'un processus EIGRP, notamment le résumé automatique des routes, les métriques de distance, la journalisation et l'ID de routeur utilisé pour envoyer des annonces d'état de liaison et d'autres mises à jour de routage. Les paramètres avancés comprennent des paramètres par défaut appropriés pour la plupart des réseaux.

Avant de commencer

Cette procédure suppose que vous ayez déjà configuré le processus EIGRP; voir Configurer le processus Core EIGRP, à la page 404.

Lorsque vous créez le processus, certaines options avancées sont activées par défaut. Vous verrez ces options activées lorsque vous modifierez l'objet EIGRP.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) du routeur virtuel global.

Étape 3 Cliquez sur l'onglet **EIGRP**.

Étape 4 Cliquez sur l'icône de modification ( ) de l'objet EIGRP.

Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) au-dessus du corps de l'objet pour ajouter toutes les autres lignes de configuration possibles.

Étape 6 La ligne **setup eigrp** *de configuration* devrait déjà être activée en tant que **setup eigrp advanced**. Si ce n'est pas le cas, cliquez sur le **signe plus (+)** à gauche de la ligne pour l'activer, puis cliquez sur la variable et sélectionnez **advanced**.

Étape 7 (Facultatif ; non recommandé.) Pour résumer automatiquement les routages sur les limites de numéro de réseau, cliquez sur le signe **plus (+)** à côté de la commande **auto-summary**.

L'activation du résumé automatique peut entraîner des problèmes de routage si vous avez des réseaux non contigus.

Par exemple, si un routeur est connecté aux réseaux 172.16.1.0, 172.16.2.0 et 172.16.3.0, et que ces réseaux prennent tous part à l'EIGRP, le processus de routage EIGRP crée l'adresse sommaire 172.16.0.0 pour ces routes. Si un routeur supplémentaire est ajouté au réseau avec les réseaux 172.16.10.0 et 172.16.11.0, et que ces réseaux prennent part à l'EIGRP, ils seront également résumés comme 172.16.0.0. Ainsi, en résumant automatiquement les routes, le trafic est acheminé vers le mauvais routeur.

Étape 8 (Facultatif ; non recommandé.) Configurez l'ID du routeur.

Cliquez sur le **signe plus (+)** pour activer la commande **router-id**, puis cliquez sur la variable et saisissez l'adresse IPv4 qui doit être utilisée lors de l'envoi des mises à jour de routeur à partir de ce périphérique. Deux routeurs dans un système autonome EIGRP ne peuvent pas avoir le même ID de routeur. Assurez-vous donc qu'il est unique dans le système.

Si vous ne spécifiez pas explicitement d'ID de routeur pour le processus, le système utilise l'adresse IP la plus élevée attribuée à une interface active. Ainsi, l'ID du routeur peut changer si vous désactivez l'interface sélectionnée ou si vous modifiez ses adresses. En attribuant explicitement un ID de routeur, vous assurez la cohérence de votre processus.

Étape 9 (Facultatif) Configurez les distances administratives pour les routes EIGRP internes et externes.

La commande suivante est activée par défaut lorsque vous configurez le processus. Si vous configurez un nouvel objet, vous devrez peut-être cliquer sur + pour activer la commande.

distance eigrp 90 170

Puisque les protocoles de routage ont des métriques basées sur des algorithmes différents de ceux des autres protocoles, il n'est pas toujours possible de déterminer le « meilleur chemin » pour deux routes vers la même destination qui ont été générées par différents protocoles de routage. La distance administrative est un paramètre de routage que le système 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.

Les distances administratives pour l'EIGRP sont comprises entre 1 et 255. Ces chiffres sont relatifs aux valeurs administratives affectées à d'autres processus de routage lorsque le système choisit les meilleures routes. En général, plus la valeur est élevée, plus l'indice de confiance est faible. Les valeurs par défaut devraient fonctionner pour la plupart des réseaux. Réglez-les si vous le souhaitez pour donner la préférence aux routes EIGRP ou si vous souhaitez réduire la probabilité que les routes EIGRP soient utilisées.

Les chiffres signifient les éléments suivants :

- Première valeur (90) : **Internal Distance** (Distance interne). La distance administrative pour les routes internes EIGRP. Les routes internes sont celles qui sont apprises d'une autre entité du même système autonome.
- Deuxième valeur (170) : **External Distance**Distance externe. La distance administrative pour les routages externes EIGRP. Les routes externes sont celles pour lesquelles le meilleur chemin est appris d'un voisin externe au système autonome.

Étape 10 La commande **default-metric** est utilisée lors de la redistribution des routes à partir d'autres processus de routage. Configurez-le uniquement si vous configurez également la redistribution. Pour de plus amples renseignements, consultez la section Configurer la redistribution des routes EIGRP, à la page 415.

Étape 11 Configurez la journalisation des voisins.

Les commandes suivantes sont activées par défaut lorsque vous configurez le processus. Si vous configurez un nouvel objet, vous devrez peut-être cliquer sur + pour activer la commande. Si vous souhaitez désactiver la journalisation, cliquez sur - pour désactiver les commandes.

- **eigrp log-neighbor-changes** active la journalisation des modifications d'adjacence des voisins EIGRP.
- **eigrp log-neighbor-warnings 10** active la journalisation des messages d'avertissement de voisin EIGRP. Le nombre est l'intervalle de temps entre les messages d'avertissement de voisin répétés, de 1 à 65535 secondes. Les avertissements répétés ne sont pas journalisés s'ils se produisent pendant cet intervalle.

Étape 12 Si vous souhaitez configurer la commande **setup stub**, consultez Configurer le processus EIGRP pour le routage de talon, à la page 405.

Étape 13 Cliquez sur **OK**.

Configurer les réseaux pour l'annonce par l'EIGRP

Utilisez la commande **network** pour identifier les réseaux et, par voie de conséquence, les interfaces qui doivent être incluses dans le 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.

Avant de commencer

Cette procédure suppose que vous ayez déjà configuré le processus EIGRP ; voir Configurer le processus Core EIGRP, à la page 404.

Créez les objets réseau qui définissent les réseaux à annoncer.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) du routeur virtuel global.

Étape 3 Cliquez sur l'onglet **EIGRP**.

Étape 4 Cliquez sur l'icône de modification ( ) de l'objet EIGRP.

Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) au-dessus du corps de l'objet pour ajouter toutes les autres lignes de configuration possibles.

Étape 6 En supposant que vous ayez déjà configuré un réseau, cliquez sur **...** > **Dupliquez** > **(Duplicate)** à côté d'une ligne **network** pour créer une nouvelle commande vide.

Si vous n'avez encore défini aucun réseau, cliquez sur le signe plus (+) à côté de la ligne vide **network** *d'objet réseau*.

Étape 7 Dans la commande **network**, cliquez sur la variable et sélectionnez l'objet qui définit un réseau qui doit être inclus dans ce système autonome.

En règle générale, il s'agirait d'un réseau directement connecté. Par exemple, si l'adresse IP de l'interface interne est 192.168.1.1/24, l'objet réseau associé à cette commande contiendra 192.168.1.0/24. Si l'objet n'existe pas encore, cliquez sur **Create New Network** (Créer un nouveau réseau) pour le créer maintenant.

Les réseaux directement connectés et statiques qui appartiennent au réseau défini sont annoncés par le processus. De plus, seules les interfaces ayant une adresse IP qui entre dans le réseau défini participent au processus de routage EIGRP.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, consultez Configurer les interfaces de routage passif EIGRP, à la page 411.

Étape 8 Si vous avez d'autres réseaux à acheminer, cliquez sur **…** > **Duplicate** > **(Dupliquer)** à gauche de la commande **network** pour en ajouter une nouvelle. Continuez à ajouter des lignes **network** jusqu'à ce que vous ayez configuré tous les réseaux pour le routage.

Étape 9 Cliquez sur **OK**.

Configurer les interfaces de routage passif EIGRP

Si vous avez une interface que vous ne souhaitez pas voir participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, vous pouvez configurer une commande **network** qui inclut le réseau auquel l'interface est associée et utiliser la commande **passive-interface** pour empêcher cette interface d'envoyer ou de recevoir des mises à jour d'EIGRP.

Par défaut, le système active la commande **no passive-interface default**, qui définit toutes les interfaces pour qu'elles soient actives, envoyant et recevant des mises à jour d'EIGRP.

La procédure suivante explique comment modifier une interface pour qu'elle soit passive.

Avant de commencer

Cette procédure suppose que vous ayez déjà configuré le processus EIGRP ; voir Configurer le processus Core EIGRP, à la page 404.

Lorsque vous créez le processus, vous ajoutez les commandes **network** pour indiquer quels réseaux doivent être acheminés à l'aide du protocole EIGRP. Pour configurer des réseaux supplémentaires à acheminer, consultez Configurer les réseaux pour l'annonce par l'EIGRP, à la page 410.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage () du routeur virtuel global.

Étape 3 Cliquez sur l'onglet **EIGRP**.

Étape 4 Cliquez sur l'icône de modification () de l'objet EIGRP.

Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) au-dessus du corps de l'objet pour ajouter toutes les autres lignes de configuration possibles.

Étape 6 Si vous modifiez un objet, la commande **configure interface passive** et son enfant, **no passive-interface default**, sont activés.

Pour un nouvel objet, cliquez sur + pour activer la commande **configure routing-interface** *des paramètres*.

Étape 7 Pour configurer les interfaces pour qu'elles soient actives par défaut, puis les rendre passives de manière sélective :

a) Dans la commande **configure routing-interface**, cliquez sur la variable et sélectionnez **passive**.

Cette action active la commande **no passive-interface default**, qui rend les interfaces EIGRP actives par défaut.

b) Cliquez sur **+** à côté de la commande **passive-interface** *d'interface*, cliquez sur la variable et sélectionnez l'interface qui doit être passive et ne pas participer aux mises à jour de routage EIGRP.

c) Cliquez sur **...** > **Cliquez sur** > **Duplicate** > **(Dupliquer)** à côté de la commande **passive-interface** *d'interface* si vous devez configurer des interfaces passives supplémentaires. Continuez jusqu'à ce que vous ayez une commande **passive-interface** pour chaque interface qui doit être passive.

Étape 8 Pour configurer les interfaces pour qu'elles soient passives par défaut, puis les rendre actives de manière sélective :

a) Dans la commande **configure routing-interface**, cliquez sur la variable et sélectionnez **active**.

Cette action active la commande **passive-interface default**, qui rend les interfaces EIGRP passives par défaut.

b) Cliquez sur **+** à côté de la commande **no passive-interface** *d'interface*, cliquez sur la variable et sélectionnez l'interface qui doit participer activement aux mises à jour de routage EIGRP.

c) Cliquez sur **...** > **Cliquez sur** > **Duplicate** > **(Dupliquer)** à côté de la commande **no passive-interface** *d'interface* si vous devez configurer des interfaces actives supplémentaires. Continuez jusqu'à ce que vous ayez une commande **no passive-interface** pour chaque interface qui doit être active.

Étape 9 Pour faire revenir une interface au comportement par défaut (passif ou actif), cliquez sur **-** à côté de la commande qui rend cette interface passive ou active. Cela supprime l'exception et fait se comporter l'interface selon l'action par défaut que vous avez définie.

Étape 10 Cliquez sur **OK**.

Configurer les voisins statiques EIGRP

Les paquets Hello EIGRP sont envoyés en tant que paquets de multidiffusion. Si un voisin EIGRP se trouve sur un réseau sans diffusion, comme dans un tunnel VPN, vous devez définir manuellement ce voisin. Lorsque vous définissez un voisin EIGRP, les paquets Hello sont envoyés à ce voisin en tant que messages unicast.

Vous n'avez pas besoin de définir les voisins statiques qui se trouvent sur des réseaux de diffusion classiques, car ces routeurs peuvent établir eux-mêmes des relations d'adjacence.

Avant de commencer

Cette procédure suppose que vous ayez déjà configuré le processus EIGRP; voir Configurer le processus Core EIGRP, à la page 404.

Déterminez l'interface par laquelle le système doit atteindre le voisin.

Vous pouvez également configurer les paramètres de journalisation pour les voisins, comme expliqué dans la section Configurer les paramètres avancés EIGRP, à la page 408.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) du routeur virtuel global.

Étape 3 Cliquez sur l'onglet **EIGRP**.

Étape 4 Cliquez sur l'icône de modification ( ) de l'objet EIGRP.

Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) pour exposer toutes les commandes, puis cliquez sur **+** pour activer la commande **neighbor**.

Étape 6 Configurez l'adresse du voisin.

neighbor *adresse IP* **interface** *interface*

- Cliquez sur *ip-address* et saisissez l'adresse IP du routeur voisin.
- Cliquez sur *interface* et sélectionnez l'interface par laquelle le système peut atteindre le routeur.

Étape 7 Si nécessaire, configurez une route statique pour le routeur voisin.

Si l'adresse IP du routeur se trouve sur le même réseau que l'interface sélectionnée, une route statique n'est pas nécessaire. Par exemple, si vous sélectionnez une interface dont l'adresse IP est 10.100.10.1/24, et l'adresse du voisin est 10.100.10.2/24, vous n'avez pas besoin de route statique.

Étape 8 Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **neighbor** pour définir un autre voisin statique. Définissez-en autant que vous le souhaitez.

Étape 9 Cliquez sur **OK**.

Contrôler la diffusion de la route par défaut candidate pour l'EIGRP

Vous pouvez contrôler l'envoi ou la réception de candidats de route par défaut à partir du processus EIGRP. Par défaut, toutes les routes candidates sont annoncées ou acceptées en fonction de vos paramètres de filtrage et de redistribution de routage.

Vous ne pouvez pas désactiver directement l'envoi ou la réception d'une route par défaut. Si vous souhaitez empêcher la diffusion de la route par défaut à partir d'EIGRP, configurez ces commandes avec une liste de contrôle d'accès standard qui refuse le réseau any-ipv4.

Avant de commencer

Cette procédure suppose que vous ayez déjà configuré le processus EIGRP ; voir Configurer le processus Core EIGRP, à la page 404.

Créez les objets de liste d'accès standard de l'interface de ligne de commande Smart dont vous avez besoin pour chaque règle de filtre. Utilisez les entrées de contrôle d'accès (ACE) pour filtrer les routages qui correspondent à l'entrée et autorisez les ACE pour les routes qui doivent être mises à jour.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) du routeur virtuel global.

Étape 3 Cliquez sur l'onglet **EIGRP**.

Étape 4 Cliquez sur l'icône de modification ( ) de l'objet EIGRP.

Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) au-dessus du corps de l'objet pour ajouter toutes les autres lignes de configuration possibles.

Étape 6 Cliquez sur le signe plus + pour activer l'une des commandes suivantes ou les deux :

- **default-information in** *acl* pour contrôler la réception des routes candidats par défaut.
- **default-information out** *acl* pour contrôler l'envoi des routes candidates par défaut.

Étape 7 Cliquez sur la variable et sélectionnez la liste de contrôle d'accès standard qui applique votre filtre.

Étape 8 Cliquez sur **OK**.

Configurer les filtres de redistribution des routes EIGRP

Vous pouvez filtrer les mises à jour de routage entrantes ou sortantes en fonction des préfixes de réseau, comme défini dans une liste de contrôle d'accès standard. Le filtrage améliore votre contrôle de la distribution des routes dans un système autonome EIGRP ou sortants vers d'autres processus de routage.

Avant de commencer

Cette procédure suppose que vous ayez déjà configuré le processus EIGRP ; voir Configurer le processus Core EIGRP, à la page 404.

Créez les objets de liste d'accès standard de l'interface de ligne de commande Smart dont vous avez besoin pour chaque règle de filtre. Utilisez les entrées de contrôle d'accès (ACE) pour filtrer les routages qui correspondent à l'entrée et autorisez les ACE pour les routes qui doivent être mises à jour.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) du routeur virtuel global.

Étape 3 Cliquez sur l'onglet **EIGRP**.

Étape 4 Cliquez sur l'icône de modification ( ) de l'objet EIGRP.

Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) pour exposer toutes les commandes, puis cliquez sur + pour activer la commande **configure filter-rules** *direction*.

Étape 6 Cliquez sur *direction* et sélectionnez **in**, pour filtrer les mises à jour entrantes, ou **out**, pour filtrer les mises à jour sortantes.

Cette action ajoute les commandes **distribute-list** à l'objet.

Étape 7 Pour les filtres entrants, vous pouvez éventuellement spécifier l'interface sur laquelle filtrer les mises à jour. Si vous ne spécifiez pas d'interface, le filtre s'applique à toutes les mises à jour reçues sur n'importe quelle interface. Cliquez sur **+** pour activer l'une des options suivantes :

- **distribute-list** *acl-name* **in**

  Sélectionnez votre objet ACL standard.

- **distribute-list** *acl-name* **in interface** *interface*

  Sélectionnez votre objet ACL standard et l'interface sur laquelle filtrer les mises à jour entrantes.

Étape 8 Pour les filtres sortants, vous pouvez éventuellement spécifier le protocole, pour limiter le filtre aux routes générées par ce processus de routage, et l'interface sur laquelle filtrer les mises à jour. Cliquez sur **+** pour activer l'une des options suivantes :

- **distribute-list** *acl-name* **out**

  Sélectionnez votre objet ACL standard.

- **distribute-list** *acl-name* **out interface** *interface*

  Sélectionnez votre objet ACL standard et l'interface sur laquelle filtrer les mises à jour sortantes.

- **distribute-list** *acl-name* **out** *protocol*

  Sélectionnez votre objet ACL standard et l'un des types de route suivants :

  - **connected**. Pour les routes établies pour les réseaux qui sont directement connectés aux interfaces du système.
  - **static**. Pour les routes statiques que vous avez créées manuellement.
  - **rip**. Pour les routes générées par RIP.

- **distribute-list** *acl-name* **out** *protocol identifier*

  Sélectionnez votre objet ACL standard et l'un des types de route suivants :

  - **ospf** *process-id*. Pour les routes générées par OSPF. Cliquez sur l'identifiant et saisissez l'ID de processus pour le processus OSPF défini sur le système.
  - **bgp** *automonous-system*. Pour les routes générées par BGP. Cliquez sur l'identifiant et saisissez le numéro de système autonome pour le processus BGP défini sur le système.

Étape 9 Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **configure filter-rules** pour définir une autre règle de filtre. Définissez-en autant que vous le souhaitez.

Étape 10 Cliquez sur **OK**.

Configurer la redistribution des routes EIGRP

Vous pouvez contrôler la redistribution des routes dans un processus EIGRP à partir d'autres protocoles de routage, des routes connectées et des routes statiques.

Avant de commencer

Il est conseillé de configurer le processus de routage à partir duquel vous redistribuerez les routes et de déployer vos modifications avant de configurer la redistribution dans EIGRP.

Si vous souhaitez appliquer une carte de routage pour affiner les routes redistribuées, créez l'objet de carte de routage Smart CLI. Les routes qui correspondent à la carte de routage sont redistribuées, et toutes les routes qui ne correspondent pas ne sont pas redistribuées.

Cette procédure suppose que vous ayez déjà configuré le processus EIGRP ; voir Configurer le processus Core EIGRP, à la page 404.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) du routeur virtuel global.

Étape 3 Cliquez sur l'onglet **EIGRP**.

Étape 4 Cliquez sur l'icône de modification ( ) de l'objet EIGRP.

Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) pour exposer toutes les commandes.

Étape 6 (Facultatif) Cliquez sur + pour activer la commande **default-metric**, qui se trouve dans le groupe de commandes **setup eigrp advanced**.

La commande **default-metric** définit les métriques à utiliser pour les routes redistribuées si vous ne configurez pas de commande **redistribute metric** spécifique pour un type de route.

default-metric *métrique de bande passante métrique de délai métrique de fiabilité bande passante effective MTU du chemin*

Cliquez sur les variables et configurez les éléments suivants. Vous devez configurer toutes les variables de métrique.

- *métrique de bande passante*. Cliquez sur la variable et saisissez la bande passante pour les connexions sur cette route de 1 à 4 294 967 295 kilo-octets par seconde.
- *delay-metric* (métrique de délai). Cliquez sur la variable et saisissez le délai pour les connexions sur la route, en unités de 10 microsecondes, de 0 à 4294967295.
- *reliability-metric (métrique de fiabilité)*. Cliquez sur la variable et saisissez la métrique de fiabilité EIGRP pour la route, de 0 à 255, où 255 indique 100 % de fiabilité. Cette métrique est ignorée, mais vous devez toujours la configurer.
- *effective-bandwidth* (bande passante effective). Cliquez sur la variable et saisissez la bande passante effective EIGRP pour la route, de 1 à 255, où 255 indique 100 % de charge. Cette métrique est ignorée, mais vous devez toujours la configurer.
- *path-MTU* (MTU du chemin). Cliquez sur la variable et saisissez l'unité de transmission maximale (MTU) du chemin, de 1 à 65 535. Cette métrique est ignorée, mais vous devez toujours la configurer.

Étape 7 Cliquez sur + pour activer la commande **configure redistribution**.

Étape 8 Cliquez sur la variable *protocol* (protocole) et sélectionnez le processus source à partir duquel vous redistribuez les routes. Vous pouvez redistribuer les routes **connected** et **static**, ou les routes générées par **bgp**, **isis**, **ospf**, ou **rip**.

Étape 9 Si vous sélectionnez un processus de routage, cliquez sur la variable *identifier* (identifiant) et saisissez la valeur requise :

- **bgp**. Saisissez le numéro du système autonome.
- **ospf**. Saisissez le numéro d'ID de processus.
- **connected**, **static**, **isis**, **rip**. Entrez **none**. Même si vous saisissez une valeur différente, elle sera ignorée.

Étape 10 (Facultatif ; IS-IS uniquement.) Dans la commande **redistribute isis route-level** *route-level*, cliquez sur la variable et choisissez si vous redistribuez les routes apprises uniquement dans une zone IS-IS (**level-1**), entre les zones IS-IS (**level-2**) ou les deux (**level-1-2**).

Étape 11 (Facultatif ; tous les protocoles.) Pour affiner les routes redistribuées en fonction d'une carte de routage, cliquez sur le signe **plus (+)** pour activer la commande **redistribute** *carte de routage*, cliquez sur la variable et sélectionnez la carte de routage qui définit vos restrictions.

Si vous n'appliquez pas de carte de routage, toutes les routes du processus (qui correspondent aux autres commandes configurées pour la redistribution) sont redistribuées.

Étape 12 (Facultatif ; tous les protocoles.) Pour affiner les mesures pour les routes redistribuées, cliquez sur **+** pour activer la commande suivante et configurer les options :

redistribute *protocol* **metric** *bandwidth-metric delay-metric reliability-metric effective-bandwidth path-MTU*

Cliquez sur les variables et configurez les valeurs, qui sont expliquées dans la commande **default-metric** ci-dessus. Vous devez configurer toutes les variables de métrique.

Étape 13 (Facultatif ; OSPF uniquement.) Les commandes suivantes sont activées par défaut lorsque vous redistribuez les routes d'un protocole OSPF. Vous pouvez cliquer sur **-** pour désactiver les commandes indésirables.

Ces commandes précisent les critères selon lesquels les routes OSPF sont redistribuées dans d'autres domaines de routage.

- **redistribute ospf match external 1**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 1.
- **redistribute ospf match external 2**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 2.
- **redistribute ospf match internal**. Routes internes à un système autonome spécifique.
- **redistribute ospf match nssa-external 1**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 1 et marquées comme Not-So-Stubby-Area (NSSA) uniquement.
- **redistribute ospf match nssa-external 2**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 2 et marquées comme Not-So-Stubby-Area (NSSA) uniquement.

Étape 14 Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **configure redistribution** pour configurer la redistribution pour un autre protocole. Configurez la redistribution pour chaque protocole qui a du sens pour votre réseau.

Étape 15 Cliquez sur **OK**.

Surveillance 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.

- **show eigrp events** [{*start end*} | **type**]

  Affiche le journal des événements EIGRP.

- **show eigrp interfaces** [*if-name*] [**detail**]

  Affiche les interfaces participant au routage EIGRP.

- **show eigrp neighbors** [**detail** | **static**] [*if-name*]

  Affiche la table des voisins EIGRP.

- **show eigrp topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  Affiche la table de topologie EIGRP.

- **show eigrp traffic**

  Affiche les statistiques de trafic EIGRP.



CHAPITRE 17

Protocole de routage BGP

BGP est utilisé pour échanger des informations de routage pour Internet et est le protocole utilisé entre les fournisseurs de services Internet (ISP). Si votre système est une passerelle vers le réseau du fournisseur de services, vous devrez peut-être mettre en œuvre BGP. Vous pouvez configurer un processus BGP sur le périphérique, pour un seul système autonome.

- À propos de BGP, à la page 419
- Configurer le protocole BGP, à la page 422
- Supervision BGP, à la page 445

À propos de BGP

BGP est un protocole de routage de systèmes inter et intra autonomes. Un système autonome est un réseau ou un groupe de réseaux soumis à une administration et à des politiques de routage communes. BGP est utilisé pour échanger des informations de routage pour Internet et est le protocole utilisé entre les fournisseurs de services Internet (ISP).

Modifications apportées à la table de routage

Les voisins BGP échangent des informations de routage complètes lors de la connexion TCP entre voisins est établie pour la première fois. Lorsque des modifications de la table de routage sont détectées, les routeurs BGP envoient à leurs voisins uniquement les routes qui ont été modifiées. Les routeurs BGP n'envoient pas de mises à jour de routage périodiques et les mises à jour de routage BGP n'annoncent que le chemin optimale vers un réseau de destination.

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.

Les routes apprises via BGP ont des propriétés utilisées pour déterminer la meilleure route vers une destination, lorsque plusieurs chemins existent vers une destination particulière. Ces propriétés sont appelées attributs BGP et sont utilisées dans le processus de sélection 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 pondération, l'attribut de préférence locale se propage dans tout le système autonome local. S'il y a plusieurs points de sortie du système autonome, le point de sortie avec l'attribut de préférence locale le plus élevé est utilisé comme point de sortie pour une route 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.
- 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.

Quand utiliser 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.

Sélection du chemin BGP

BGP peut recevoir plusieurs annonces pour la même route provenant de différentes sources. BGP sélectionne un seul chemin comme meilleur chemin. Lorsque ce chemin est sélectionné, BGP le met dans la table de routage IP et propage le chemin à ses voisins. BGP utilise les critères suivants, dans l'ordre présenté, pour sélectionner un chemin pour une destination :

- Si le chemin précise un saut suivant inaccessible, supprimez la mise à jour.
- Privilégiez le chemin avec la pondération la plus élevée.
- 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.
- 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).
- 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.
- 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 421.
- Si les deux chemins sont externes, privilégiez le chemin qui a été reçu en premier (le plus ancien).
- 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.
- Privilégiez le chemin qui provient de l'adresse du voisin le plus bas.

Chemins multiples BGP

Les chemins BGP multiples permettent l'installation dans la table de routage IP de plusieurs chemins BGP à coût égal vers le même préfixe de destination. Le trafic vers le préfixe de destination est ensuite partagé sur tous les chemins installés.

Ces chemins sont installés dans le tableau avec le meilleur chemin pour le partage de la charge. Les chemins multiples de 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 avoir ces caractéristiques égales aux caractéristiques du 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 de BGP)

Certaines fonctionnalités de chemins multiples de BGP appliquent des exigences supplémentaires aux candidats aux chemins multiples :

- Le chemin doit être appris d'un voisin externe ou d'un voisin externe à la confédération (eBGP).
- La métrique IGP au saut suivant de 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 de BGP doit être égale à la métrique du meilleur chemin IGP, sauf si le routeur est configuré pour les chemins multiples iBGP à coût inégal.

BGP insère jusqu'à *n* derniers chemins reçus de candidats aux chemins multiples dans la table de routage IP, *n* étant le nombre de routes à installer dans la table de routage, comme spécifié lorsque vous configurez BGP multi-chemins. La valeur par défaut, lorsque les chemins multiples sont désactivé, est 1.

Pour l'équilibrage de charge à coût inégal, vous pouvez également utiliser la bande passante du lien BGP.



Remarque Le prochain-saut-self équivalent est effectué sur le meilleur chemin sélectionné parmi les chemins multiples eBGP avant qu'il ne soit transmis aux homologues internes.

Configurer le protocole BGP

Les rubriques suivantes expliquent comment configurer BGP.

Configurer les paramètres globaux BGP

Si vous configurez BGP, les paramètres globaux s'appliquent à tous les routeurs virtuels, si vous utilisez des routeurs virtuels. Il existe des paramètres BGP supplémentaires que vous configurez pour définir le processus BGP. Lorsque vous utilisez des routeurs virtuels, vous pouvez créer un processus BGP distinct pour chaque routeur virtuel.

Avant de commencer

Après avoir créé l'objet des paramètres globaux BGP, vous pouvez le supprimer si vous n'en avez plus besoin. Modifiez simplement l'objet en suivant cette procédure, mais cliquez sur le bouton **Delete BGP Global Settings Object** (Supprimer l'objet des paramètres globaux BGP) au bas de la boîte de dialogue.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis cliquez sur le résumé du **Routing** (Routage).

Étape 2 Sur la page de routage principale ou de routeurs virtuels, cliquez sur le bouton **BGP Global Settings** (Paramètres globaux BGP .

Si vous affichez un routeur virtuel, vous devez revenir à la liste principale des routeurs virtuels.

Étape 3 Si vous n'avez pas encore configuré l'objet de paramètres globaux BGP, cliquez sur **Create BGP Global Settings Object** (Créer un objet de paramètres globaux BGP).

Étape 4 (Facultatif) Vous pouvez modifier le nom de l'objet ou saisir une description pour l'objet. Le nom de l'objet par défaut est BgpGeneralSettings.

Étape 5 Configurez au moins les paramètres de base suivants :

- **router bgp** *as-number*. Cliquez sur *as-number* et saisissez le numéro de système autonome (AS) pour le processus BGP. Le numéro de système autonome peut être compris entre 1 et 4294967295 ou entre 1.0 et 6553565535. Le numéro de système autonome est une valeur attribuée de façon unique qui identifie chaque réseau sur Internet. Le système prend en charge les notations asplain et asdot, telles que définies dans la RFC 5396.
- **log-neighbor-changes** *state (État)*. Cliquez sur *state (État)* et sélectionnez enable (Activer) ou disable (Désactiver). Lorsque cette option est activée, ce qui est recommandé, les modifications de voisin BGP (montées ou descentes) et les réinitialisations sont journalisées. Cela aide à résoudre les problèmes de connectivité du réseau et à mesurer la stabilité du réseau.
- **transport path-mtu-discovery** *state (État)*. Cliquez sur *state (État)* et sélectionnez enable (Activer) ou disable (Désactiver). Lorsque cette option est activée, ce qui est recommandé, le système détermine la taille maximale d'unité de transmission (MTU) sur le chemin réseau entre deux hôtes IP, puis tire parti du chemin présentant le MTU le plus élevé. Cela permet d'éviter la fragmentation IP.
- **fast-external-fallover** *state (État)*. Cliquez sur *state (État)* et sélectionnez enable (Activer) ou disable (Désactiver). Lorsque cette option est activée, ce qui est recommandé, le système utilise le basculement externe rapide pour les sessions d'homologation BGP avec des homologues externes directement connectés. La session est immédiatement réinitialisée si la liaison est interrompue. Si vous désactivez le basculement externe rapide BGP, le processus de routage BGP attendra l'expiration de la minuterie de rétention par défaut (3 keepalives) pour réinitialiser la session d'homologation.

- **enforce-first-as** *state (État)*. Cliquez sur *state (État)* et sélectionnez enable (Activer) ou disable (Désactiver). Lorsque cette option est activée, ce qui est recommandé, le système refuse les mises à jour entrantes reçues des homologues eBGP qui ne répertorient pas leur numéro de système autonome comme premier segment dans l'attribut AS_PATH. L'activation de cette commande empêche un homologue mal configuré ou non autorisé de détourner le trafic (en usurpant le routeur local) en annonçant une route comme si elle provenait d'un autre système autonome.

Étape 6 (Facultatif) Cliquez sur le lien **Show Disabled (Afficher les éléments désactivés** au-dessus du corps de l'objet pour ajouter toutes les autres lignes de configuration possibles.

Vous pouvez activer les options suivantes en cliquant sur le signe plus + à gauche de l'option.

- **bgp asnotation dot**. Modifie l'affichage par défaut et le format de correspondance des expressions régulières pour les numéros de système autonome BGP à 4 octets, d'asplain (valeurs décimales) à asdot (notation avec point). Le système utilise asplain comme format d'affichage par défaut pour les numéros de système autonome, mais vous pouvez configurer des numéros de système autonome de 4 octets aux formats asplain et asdot, même si vous n'activez pas cette commande.

  En outre, le format par défaut pour la correspondance des numéros de système autonome à 4 octets dans les expressions régulières est asplain. Vous devez donc vous assurer que toutes les expressions régulières correspondant aux numéros de système autonome à 4 octets sont écrites au format asplain si vous n'activez pas cette commande.

- **bgp scan time 60**. Cliquez sur le numéro et saisissez l'intervalle d'analyse des routeurs BGP pour la validation du saut suivant, de 5 à 60 secondes. La valeur par défaut est de 60 secondes.

- **configure nexthop trigger** *state (État)*. Cliquez sur *state (État)* et sélectionnez **enable** ou **disable**. Le suivi des adresses de saut suivant de BGP est basé sur les événements. Les préfixes de BGP sont automatiquement suivis lorsque les sessions d'homologation sont établies. Les modifications apportées au prochain saut sont rapidement signalées à BGP, car elles sont mises à jour dans la base d'informations de routage (RIB). Cette optimisation améliore la convergence globale de BGP en réduisant le temps de réponse aux modifications de saut suivant pour les routes installées dans le RIB. Lorsqu'un calcul du meilleur chemin est exécuté entre les cycles d'analyse BGP, seules les modifications sont traitées et suivies. Si vous activez le suivi des adresses du saut suivant, les commandes suivantes sont ajoutées. Notez que si vous ne configurez pas les options générales dans un nouvel objet, la valeur par défaut est d'activer cette fonctionnalité.

  - **bgp nexthop trigger enable**. Le suivi des adresses de saut suivant BGP améliore considérablement le temps de réponse de BGP. Cependant, les homologues du protocole de passerelle intérieure (IGP) instables peuvent introduire une instabilité dans le protocole BGP. Nous vous recommandons de réduire de manière dynamique les sessions d'homologation IGP instables afin de limiter l'impact possible sur BGP.

  - **bgp nexthop trigger delay 5**. Cliquez sur le numéro pour modifier l'intervalle de délai entre les marches de la table de routage pour le suivi de l'adresse du saut suivant de BGP. Vous pouvez augmenter les performances du suivi des adresses du saut suivant de BGP en réglant l'intervalle de délai entre les marches complètes de la table de routage pour qu'il corresponde aux paramètres de réglage de l'IGP. L'intervalle de délai par défaut est de 5 secondes, qui est une valeur optimale pour un IGP à réglage rapide. Dans le cas d'un IGP qui converge plus lentement, vous pouvez modifier l'intervalle de retard à 20 secondes ou plus, en fonction du temps de convergence de l'IGP. Vous pouvez définir le délai de 0 à 100 secondes.

- **bgp aggregate-timer 30**. Cliquez sur le numéro pour définir l'intervalle auquel les routes BGP seront agrégées, de 6 à 60 secondes. La valeur par défaut est de 30 secondes.

- **bgp router-id** *router-id*. Cliquez sur *router-id* et saisissez l'adresse IPv4 qui doit être utilisée comme ID routeur global. Cet ID est utilisé pour tout processus BGP dans un routeur virtuel qui ne spécifie pas lui-même d'ID de routeur. Si vous n'activez pas cette commande, l'ID de routeur est défini selon l'adresse IP la plus élevée sur une interface physique attribuée au routeur virtuel. Utilisez cette commande pour vous assurer que l'ID du routeur reste stable.
- **bgp maxas-limit** *value (Valeur)*. Cliquez sur *value (Valeur)* et saisissez le nombre maximal de numéros de système autonome dans l'attribut chemin AS du message de mise à jour de BGP, de 1 à 254. Un attribut chemin AS est une séquence de numéros AS intermédiaires entre les routeurs source et destination qui forment une route dirigée pour les paquets. Le système supprime les routes qui ont un certain nombre de systèmes autonomes dans le chemin AS qui dépassent la valeur spécifiée. En plus de définir la limite du nombre de numéros de système autonome dans le segment de chemin AS, la commande limite le nombre de segments de chemin AS à dix. Si vous n'activez pas cette commande, aucune route n'est rejetée.

Étape 7 (Facultatif) Configurer les options avancées.

Cliquez sur le lien **Show Disable**d (Afficher la désactivation) si nécessaire pour exposer la commande suivante. Lors de la modification des paramètres, les ensembles d'options **timers** et **bestpath** sont affichés, car ils ont des valeurs par défaut qui sont activées même si vous ne les définissez pas explicitement.

configure bgp advanced *advanced-option (Option avancée)*

Cliquez sur *advanced-option (Option avancée)* et sélectionnez l'une des options suivantes. Vous pouvez configurer toutes ces options en cliquant sur ... dans la colonne de gauche et en sélectionnant **Duplicate (Dupliquer)**.

- **timers**. Configure les minuteurs utilisés lors de la communication avec les routeurs voisins BGP.

  timers bgp 60 180 0

  - Première valeur (60 par défaut) : **Intervalle Keepalive**. Cliquez sur le numéro et saisissez la fréquence à laquelle le système envoie des messages Keepalive à son voisin BGP, de 0 à 65 535 secondes. Nous vous recommandons de ne pas spécifier 20 ou moins, sinon vous pourriez trouver des routes oscillant inutilement.
  - Deuxième valeur (par défaut 180) : **Temps d'attente**. Cliquez sur le nombre et saisissez la durée d'attente du système après n'avoir pas reçu de message Keepalive avant de déclarer un voisin de BGP mort, de 0 à 65 535 secondes.
  - Troisième valeur (0 par défaut) : **Minimum Hold Time** (Délai de rétention minimal). Cliquez sur le nombre et spécifiez le délai de rétention minimal acceptable configuré sur le voisin BGP. Le délai de rétention minimal acceptable doit être inférieur ou égal à l'intervalle spécifié comme temps de rétention pour ce système. La valeur doit être comprise entre 0 et 65 535.

- **bestpath**. Configure les options utilisées dans l'algorithme de sélection du meilleur chemin de BGP. La commande **bgp default local-preference** est configurée par défaut, mais vous pouvez ajouter les autres commandes en cliquant sur le **signe plus (+)** pour la commande.
  - **bgp default local-preference 100**. Cliquez sur le numéro et saisissez une valeur qui indique la préférence de ce système par rapport aux autres routeurs dans le BGP AS, 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. Cet attribut est échangé uniquement entre les homologues iBGP et est utilisé pour déterminer la politique locale.

- **bgp always-compare-med**. 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. Par défaut, le système ne compare pas le MED pour les chemins des voisins dans différents systèmes autonomes.
- **bgp bestpath compare-routerid**. Utilisez l'ID du routeur comme disjoncteur de liaison pour la meilleure sélection de chemin lorsque deux routes identiques sont reçues de deux homologues différents (tous les attributs sont les mêmes, à l'exception de l'ID du routeur). Lorsque cette commande est activée, l'ID de routeur le plus bas sera sélectionné comme meilleur chemin lorsque tous les autres attributs sont égaux. Sinon, la première voie de routage reçue est utilisée.
- **bgp deterministic-med**. Sélectionnez le meilleur chemin MED annoncé par le système autonome voisin.
- **bgp bestpath med missing-as-worst**. Définissez un chemin avec un attribut MED manquant comme chemin le moins préféré. Par défaut, le système considère la voie de routage avec un MED manquant comme la meilleure voie de routage.

- **graceful-restart**. Configurez le redémarrage progressif pour les systèmes dans une configuration à haute disponibilité ou en grappe.
  - **bgp graceful-restart**. Active le redémarrage progressif pour un transfert sans interruption. Grâce au redémarrage progressif, le système peut annoncer la capacité de maintenir l'état de transfert pour un groupe d'adresses pendant le redémarrage.
  - **bgp graceful-restart restart-time 120**. Cliquez sur le nombre et saisissez la période maximale pendant laquelle le système attendra qu'un voisin compatible avec le redémarrage progressif revienne au fonctionnement normal après un événement de redémarrage, de 1 à 3 600 secondes. La valeur par défaut est de 120 secondes.
  - **bgp graceful-restart stalepath-time 360**. Cliquez sur le nombre et saisissez la période maximale pendant laquelle le système conservera les chemins périmés pour un homologue qui redémarre, de 1 à 3 600 secondes. Tous les chemins obsolètes sont supprimés après l'expiration de cette minuterie. La valeur par défaut est 360 secondes.

Étape 8 Cliquez sur **OK**.

Configurer le processus de BGP

Après avoir configuré les paramètres globaux de BGP, vous pouvez configurer le processus BGP. Si vous utilisez des routeurs virtuels, vous pouvez configurer un processus distinct pour chaque routeur virtuel. Vous pouvez configurer au plus un processus BGP pour le système ou par routeur virtuel.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **Routing** (Routage) dans le résumé.

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez le BGP.

Étape 3 Cliquez sur l'onglet **BGP**.

Étape 4 Effectuez l'une des opérations suivantes :

- Pour créer un processus, cliquez sur le signe plus **(+** ou cliquez sur le bouton **Create BGP Object** (Créer un objet BGP).
- Cliquez sur l'icône de modification () de l'objet que vous souhaitez modifier. Notez que lorsque vous modifiez un objet, vous pouvez voir des lignes que vous n'avez pas configurées directement. Ces lignes sont affichées pour vous montrer les valeurs par défaut en cours de configuration.

Si vous n'avez plus besoin d'un processus, cliquez sur l'icône de la corbeille pour supprimer l'objet.

Étape 5 Saisissez un nom pour l'objet et, facultativement, une description.

Étape 6 Configurez les paramètres minimaux pour le processus :

- **router bgp** *as-number*. Cliquez sur *as-number* et saisissez le même numéro de système autonome (AS) pour le processus BGP que vous avez spécifié dans les paramètres globaux. Le numéro de système autonome peut être compris entre 1 et 4294967295 ou entre 1.0 et 6553565535. Le numéro de système autonome est une valeur attribuée de façon unique qui identifie chaque réseau sur Internet. Le système prend en charge les notations asplain et asdot, telles que définies dans la RFC 5396.
- **configure address-family** *ip-protocol*. Cliquez sur *ip-protocol* et sélectionnez IPv4 ou IPv6. Si vous utilisez des routeurs virtuels, vous pouvez configurer IPv6 pour le routeur global uniquement. Vous pouvez configurer IPv4 pour n'importe quel routeur virtuel. La sélection d'une option ajoute les commandes **address-family ipv4 unicast** ou **address-family ipv6 unicast**, ainsi que la commande suivante que vous devez configurer :
  - **configure address-family {ipv4 | ipv6}** *settings (paramètres)*. Cliquez sur settings (paramètres) et sélectionnez **general** ou **advanced**. Vous devez configurer au moins une commande sous ces options pour avoir un processus minimal, mais cela ne sera pas suffisant pour un processus significatif.

Étape 7 Cliquez sur **Show Disabled** (Afficher désactivé) et personnalisez le processus pour qu'il fonctionne correctement dans votre réseau.

Tant que vous configurez un ensemble minimal de commandes, comme expliqué ci-dessus, vous pouvez enregistrer l'objet et personnaliser les paramètres de processus ultérieurement. Les rubriques suivantes expliquent les différents ensembles d'options. Vous devez au minimum configurer les paramètres réseau pour identifier les réseaux pour lesquels le processus distribuera les routes. Les paramètres généraux et les paramètres avancés ont des valeurs de commande par défaut qui sont appropriées dans la plupart des cas.

- Configurer les paramètres généraux BGP, à la page 428
- Configurer les paramètres avancés BGP, à la page 429
- Configurer les réseaux pour l'annonce par le BGP, à la page 431
- Configurer l'injection de route BGP, à la page 432
- Configurer les paramètres d'adresse d'association BGP, à la page 433
- Configurer les paramètres de filtre de BGP pour IPv4, à la page 435
- Configurer les voisins BGP, à la page 436
- Configurer la redistribution du routage BGP à partir d'autres protocoles de routage, à la page 443

Étape 8 (Facultatif) Configurez l'ID de routeur pour ce processus.

Vous pouvez configurer l'ID de routeur à utiliser pour le processus BGP dans les paramètres globaux de BGP. Vous pouvez également le configurer dans l'objet de processus. Tout ID de routeur configuré dans l'objet de processus remplace l'ID de routeur global. Cela permet de remplacer facilement la valeur globale pour des routeurs virtuels spécifiques.

Cliquez sur **Show Disabled** (Afficher désactivé) si la commande suivante ne s'affiche pas, puis cliquez sur le signe plus + à côté pour activer la commande.

- **bgp router-id** *router-id*. Cliquez sur *router-id* et saisissez l'adresse IPv4 qui doit être utilisée comme identifiant de routeur pour ce processus. Si vous n'activez pas cette commande, l'ID du routeur est défini selon l'ID du routeur global ou selon l'adresse IP la plus élevée sur une interface physique attribuée au routeur virtuel. Utilisez cette commande pour vous assurer que l'ID du routeur reste stable.

Étape 9 Cliquez sur **OK**.

Configurer les paramètres généraux BGP

Les paramètres généraux définissent les distances administratives, les minuteurs et, pour IPv4 uniquement, le suivi de l'adresse du saut suivant. Ces options ont des valeurs par défaut appropriées à la plupart des réseaux.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **Routing** (Routage) dans le résumé.

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez le BGP.

Étape 3 Cliquez sur l'onglet **BGP**.

Étape 4 Ajoutez ou modifiez l'objet de processus BGP.

Étape 5 Recherchez la ligne **configure address-family ipv4** ou **ipv6**. Si l'option **general** est déjà sélectionnée, passez à l'étape suivante. Cependant :

- Si la variable *settings* (paramètres) est toujours affichée, cliquez dessus et sélectionnez **general**.
- Si vous avez déjà configuré les options générales, cliquez sur le bouton **...** à gauche de la commande et sélectionnez **Duplicate** (Dupliquer). Ensuite, cliquez sur *settings* (paramètres) et sélectionnez **General**

Étape 6 Configurez les commandes suivantes :

- **distance bgp 20 200 200**. Configure les distances administratives pour BGP, de 1 à 255. Ces chiffres sont relatifs aux valeurs administratives affectées à d'autres processus de routage lorsque le système choisit les meilleures routes. En général, plus la valeur est élevée, plus l'indice de confiance est faible. Utilisez cette commande si un autre protocole est connu pour être en mesure de fournir une meilleure route à un nœud que celle qui a été réellement apprise par le BGP externe (eBGP), ou si certaines routes internes doivent être préférées par BGP. Les routages d'une distance de 255 ne sont pas installés dans la table de routage. Les chiffres signifient les éléments suivants :
  - Première valeur (20 par défaut) : **External Distance** (Distance externe). Cliquez sur le nombre, puis saisissez la distance administrative pour les routes BGP externes. Les routes sont externes lorsqu'elles sont apprises à partir d'un système autonome externe.

- Deuxième valeur (200 par défaut) : **Internal Distance** (Distance interne). Cliquez sur le nombre, puis saisissez la distance administrative pour les routes BGP internes. Les routes sont internes lorsqu'elles sont apprises de l'homologue dans le système autonome local. La modification de la distance administrative des routes de BGP internes est considérée comme dangereuse et n'est pas recommandée. Une configuration incorrecte peut introduire des incohérences dans les tables de routage et interrompre le routage.
- Troisième valeur (200 par défaut) : **Local Distance** (Distance locale). Cliquez sur le nombre, puis saisissez la distance administrative pour les routes BGP locales. Les routes locales sont destinées aux réseaux répertoriés avec une commande **network** dans le processus de routage de BGP, c'est-à-dire les réseaux annoncés par le processus ou pour les réseaux qui sont redistribués au BGP à partir d'un autre processus.

Étape 7 Cliquez sur **OK**.

Configurer les paramètres avancés BGP

Utilisez les paramètres avancés pour configurer diverses options qui ne sont nécessaires que dans des circonstances particulières. La plupart de ces options sont désactivées par défaut.

Avant de commencer

Si vous prévoyez de configurer la commande **table-map**, vous devez d'abord vous rendre à la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)** et créer l'objet de carte de routage Smart CLI requis par la commande.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **Routing** (Routage) dans le résumé.

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez le BGP.

Étape 3 Cliquez sur l'onglet **BGP**.

Étape 4 Ajoutez ou modifiez l'objet de processus BGP.

Étape 5 Recherchez la ligne **configure address-family ipv4** ou **ipv6**. Si l'option **advanced** est déjà sélectionnée, passez à l'étape suivante. Cependant :

- Si la variable *settings* (paramètres) est toujours affichée, cliquez dessus et sélectionnez **advanced**.
- Si vous avez déjà configuré les options générales, clique sz sur le bouton **...** à gauche de la commande et sélectionnez **Duplicate** (Dupliquer). Ensuite, cliquez sur *settings* (paramètres) et sélectionnez **Advanced**

Étape 6 Configurez les commandes suivantes. Vous devez cliquer sur **Show Disabled** (Afficher désactivé) pour voir tout sauf la première commande lors de la création initiale de l'objet.

Cliquez sur le signe plus **+)** pour une commande afin de l'activer.

- **bgp redistribute-internal**. Configurez la redistribution d'iBGP dans un protocole de passerelle intérieure (IGP), tel que EIGRP ou OSPF. Faites preuve de prudence lors de la redistribution d'iBGP dans un IGP.

Utilisez les instructions IP prefix-list et route-map afin de limiter le nombre de préfixes pouvant être redistribués. a redistribution d'une table de routage BGP non filtrée dans un IGP peut avoir un effet néfaste sur le fonctionnement normal du réseau IGP. Cette commande est activée par défaut, vous devez donc cliquer sur le bouton - pour la désactiver.

- **bgp suppress-inactive**. Empêchez les routes qui ne sont pas installées dans le RIB (routes inactives) d'être annoncées aux homologues. Par défaut, BGP affiche les routes inactives. Notez que BGP marque les routes qui ne sont pas installées dans le RIB avec un indicateur de défaillance du RIB. Cet indicateur apparaîtra également dans la sortie de la commande **show bgp** ; par exemple, Rib-Failure (17). Cet indicateur ne signale pas une erreur ou un problème avec la route ou avec le RIB.
- **auto-summary**. (IPv4 uniquement.) Résumez automatiquement les routes de sous-réseau en routes de niveau réseau. La récapitulation de routage réduit la quantité d'informations de routage dans les tables de routage. Désactivez la récapitulation automatique si vous devez effectuer le routage entre des sous-réseaux déconnectés. Lorsque la récapitulation automatique est désactivée, les sous-réseaux sont annoncés.
- **synchronization**. Activez la synchronisation entre BGP et votre système IGP (Interior Gateway Protocol), comme OSPF. Généralement, un interlocuteur BGP n'annonce pas de routage à un voisin externe, sauf si cette voie de routage est locale ou existe dans l'IGP. Cette fonctionnalité permet aux routeurs et aux serveurs d'accès d'un système autonome d'avoir la voie de routage avant que le BGP ne le mette à la disposition d'autres systèmes autonomes. Utilisez cette commande si les autres routeurs du système autonome n'utilisent pas BGP.
- **table-map** *de carte de routage options*. (IPv4 uniquement.) Appliquez une carte de routage qui définit des métriques, une valeur de balise ou un indice de trafic pour les routes mises à jour dans la table de routage BGP, ou qui contrôle si les routes sont téléchargées dans le RIB. Cliquez sur *route-map* (carte de routage) et sélectionnez l'objet Smart CLI qui définit la carte de routage. Dans la carte de routage, vous pouvez utiliser des clauses match pour les listes d'accès IP, les chemins du système autonome, les communautés, les listes de préfixes et le prochain saut.

  Vous pouvez déterminer comment la carte de routage est utilisée en cliquant sur *options* et en choisissant soit vide, soit **filter** :

  - Si vous ne sélectionnez pas **filter**, le système utilise la carte de routage pour définir certaines propriétés d'une route avant que celle-ci ne soit installée dans le RIB. Le routage est toujours téléchargé, qu'il soit autorisé ou non par la carte de routage.
  - Si vous sélectionnez **filter**, la carte de routage contrôle également si la route BGP est téléchargée dans le RIB. Seules les routes autorisées dans la carte de routage sont téléchargées ; les routes refusées ne le sont pas.

- **default-information originate**. Configurez BGP pour annoncer une route par défaut (réseau 0.0.0.0). La configuration de la commande **default-information originate** est similaire à la configuration de la commande **network**. La commande **default-information originate**, cependant, exige la redistribution explicite de la route 0.0.0.0, que vous devez également configurer dans cet objet. La commande **network** exige uniquement que la route 0.0.0.0 soit présente dans la table de routage de l'IGP (Interior Gateway Protocol), comme OSPF. Pour cette raison, la commande **network** est préférable pour distribuer une route par défaut.
- **maximum paths 1**. Contrôlez le nombre maximal de routes BGP parallèles pouvant être installées dans une table de routage, de 1 à 8. Utilisez cette commande pour configurer le partage de charge multipath à coût égal ou inégal pour les sessions de peering BGP. Pour qu'une route soit installée comme multipath dans la table de routage BGP, elle ne doit pas avoir un prochain saut identique à celui d'une autre route

déjà installée. Le processus de routage BGP annoncera tout de même un meilleur chemin aux homologues BGP lorsque le partage de charge multipath est configuré. Pour les routes à coût égal, le chemin provenant du voisin dont l'ID de routeur est le plus bas est annoncé comme le meilleur chemin.

Pour configurer le partage de charge multipath à coût égal pour BGP, tous les attributs de chemin doivent être identiques. Les attributs de chemin comprennent le poids, la préférence locale, le chemin du système autonome (l'attribut complet et non seulement sa longueur), le code d'origine, le discriminateur de sortie multiple (MED) et la distance de l'IGP (Interior Gateway Protocol).

- **maximum paths ibgp 1**. Contrôlez le nombre maximal de routes BGP internes pouvant être installées dans la table de routage, de 1 à 8. Les considérations pour l'iBGP multipath sont les mêmes que celles décrites pour la commande **maximum paths** ci-dessus.

Étape 7 Cliquez sur **OK**.

Configurer les réseaux pour l'annonce par le BGP

Vous devez définir les réseaux à annoncer par le processus de routage BGP.

Avant de commencer

Créez les objets réseau qui définissent les réseaux à annoncer. Vous pouvez définir des réseaux IPv4 ou IPv6, ou les deux, selon les gammes d'adresses que vous configurez pour BGP.

Si les objets réseau spécifient de grands espaces réseau, vous pouvez également créer des cartes de routage à appliquer à l'objet réseau pour filtrer les sous-réseaux dans l'espace plus grand que vous ne souhaitez pas annoncer. Seules les routes qui correspondent aux spécifications de la carte de routage sont annoncées. Utilisez Smart CLI (interface de ligne de commande Smart) pour créer l'objet de carte de routage.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **Routing** (Routage) dans le résumé.

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez le BGP.

Étape 3 Cliquez sur l'onglet **BGP**.

Étape 4 Ajoutez ou modifiez l'objet de processus BGP.

Les commandes de réseau se trouvent dans les ensembles de commandes sous la commande **configure address family ipv4** ou **ipv6**. Vous devez configurer la famille d'adresses pour configurer les réseaux à annoncer.

La commande **network** dans chaque groupe d'adresses doit préciser des adresses qui correspondent à la famille d'adresses que vous configurez.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) pour exposer toutes les commandes, puis cliquez sur **+** pour activer la commande **network** ou **network route-map** et configurez les options :

- *objet réseau*. Cliquez sur la variable et sélectionnez l'objet réseau qui définit les réseaux à annoncer : adresse et masque réseau IPv4 ou adresse et préfixe réseau IPv6.

- **route-map** *carte de routage*. Cliquez sur la variable et sélectionnez la carte de routage qui doit être appliquée à l'objet réseau pour filtrer les adresses dans la plage qui doivent être annoncées.
- (Facultatif; IPv6 uniquement.) *nom de préfixe*. Cliquez sur la variable et saisissez le nom d'un préfixe DHCPv6 pour annoncer le préfixe. Si vous configurez cette option, l'objet réseau agit comme un sous-réseau pour le préfixe. Pour utiliser cette option, vous devez activer le client de délégation de préfixe DHCPv6, ce qui nécessite d'utiliser FlexConfig pour ajouter la commande **ipv6 dhcp client pd** à une interface en mode de configuration d'interface.

Étape 6 Vous pouvez cliquer sur **...** > **Duplicate (Dupliquer)** à côté de la commande **network** ou **network route-map** pour configurer des réseaux supplémentaires à annoncer.

Étape 7 Cliquez sur **OK**.

Configurer l'injection de route BGP

Vous pouvez configurer l'injection de route conditionnelle pour injecter des routes plus spécifiques dans une table de routage BGP. L'injection de route conditionnelle vous permet de créer un préfixe plus spécifique dans une table de routage BGP sans correspondance correspondante. Une route parente valide doit exister pour tous les préfixes injectés. Seuls les préfixes égaux ou plus spécifiques que la route agrégée (préfixe existant) peuvent être injectés.

Avant de commencer

Vous devez créer les cartes de routage nécessaires pour définir les préfixes. Ces cartes de routage doivent respecter les exigences expliquées dans la procédure.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **Routing** (Routage) dans le résumé.

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez le BGP.

Étape 3 Cliquez sur l'onglet **BGP**.

Étape 4 Ajoutez ou modifiez l'objet de processus BGP.

Les commandes d'injection de route se trouvent dans les ensembles de commandes sous la commande **configure address family ipv4** ou **ipv6**. Vous devez configurer la famille d'adresses pour configurer les réseaux à annoncer.

Étape 5 Cliquez sur **Show Disabled** (Afficher les éléments désactivés) pour exposer toutes les commandes, puis cliquez sur **+** pour activer la commande **bgp inject-map**.

Étape 6 Configurez les propriétés des commandes :

- **inject-map** *inject-map*. Cliquez sur la variable et sélectionnez la carte de routage qui définit les préfixes à créer et à installer dans la table de routage. Les préfixes injectés sont installés dans le RIB de BGP local. Une route parente valide doit exister; seuls les préfixes égaux ou plus spécifiques que la route agrégée (préfixe existant) peuvent être injectés. La carte de routage doit utiliser une liste de préfixes pour préciser les routes à injecter.

- **exist-map** *exist-map*. Cliquez sur la variable et sélectionnez la carte de routage qui définit le préfixe que le locuteur BGP doit suivre. Cette carte de routage doit utiliser des listes de préfixes pour spécifier le préfixe agrégé ainsi que la source de routage. La source de routage serait un routeur, par exemple, 10.2.1.1/32, plutôt qu'un sous-réseau.
- *options*. Au besoin, cliquez sur la variable et sélectionnez **copy-attributes**. Cette option configure le préfixe injecté pour qu'il hérite des mêmes attributs que la route agrégée. Si vous ne sélectionnez pas ce mot-clé, le préfixe injecté utilisera les attributs par défaut pour les routes d'origine locale.

Étape 7 Vous pouvez cliquer sur **...** > **Duplicate (Dupliquer)** à côté de la commande **bgp inject-map** pour configurer des règles supplémentaires d'injection de routes.

Étape 8 Cliquez sur **OK**.

Configurer les paramètres d'adresse d'association BGP

Les voisins BGP stockent et échangent des informations de routage, et la quantité d'informations de routage augmente à mesure que davantage de haut-parleurs BGP sont configurés. L'agrégation de routes consiste à combiner les attributs de plusieurs routes différentes de sorte qu'une seule route soit annoncée. Les préfixes d'association utilisent le principe de routage interdomaine sans classe (CIDR) pour combiner des réseaux contigus en un ensemble d'adresses IP sans classe qui peut être résumé dans des tableaux de routage. Par conséquent, moins de routages doivent être annoncés.

Si vous configurez une route agrégée sans mot clé sur la commande, le système crée une entrée agrégée dans la table de routage BGP si des routes BGP plus spécifiques sont disponibles dans la plage spécifiée. (Un préfixe plus long qui correspond à l'agrégat doit exister dans la base d'informations de routage (RIB).) La route agrégée sera annoncée comme provenant de votre système autonome et aura l'attribut d'agrégation atomique pour afficher que les informations peuvent être manquantes. L'attribut d'agrégation atomique est défini sauf si vous spécifiez le mot-clé **as-set**.

La procédure suivante explique comment configurer l'agrégation de routes spécifiques en une seule route.

Avant de commencer

Si vous souhaitez appliquer des cartes de routage pour affiner les routes agrégées ou les attributs définis sur la route agrégée, créez les objets de carte de routage Smart CLI.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **Routing** (Routage) dans le résumé.

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez le BGP.

Étape 3 Cliquez sur l'onglet **BGP**.

Étape 4 Ajoutez ou modifiez l'objet de processus BGP.

Les commandes d'agrégation se trouvent dans les ensembles de commandes sous la commande **configure address family ipv4** ou **ipv6**. Vous devez configurer la famille d'adresses pour configurer l'agrégation.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) pour exposer toutes les commandes, puis cliquez sur **+** pour activer la commande **configure aggregate-address**.

Étape 6 Cliquez sur la variable *map-type* et sélectionnez les types de carte de routage que vous souhaitez appliquer à cette route agrégée particulière.

Cette option détermine simplement quels paramètres sont inclus dans la commande **aggregate-address** qui seront ajoutés à l'objet. Vous pouvez appliquer jusqu'à 3 cartes de routage distinctes, pour supprimer les routes de l'agrégation, pour annoncer les routes et pour définir les attributs à appliquer à la route agrégée.

- Sélectionnez **no-map** si vous n'avez pas besoin d'appliquer de carte de routage.
- Sélectionnez **all** si vous souhaitez appliquer les cartes de routage pour les trois options.
- Sélectionnez les combinaisons de mots clés appropriées si vous souhaitez appliquer une ou deux cartes, mais pas toutes : **suppress-map**, **advertise-map**, **attribute-map**, **suppress-advertise**, **suppress-attribute** , **advertise-attribute** .

Étape 7 Configurez les propriétés de la route à agréger.

Voici une liste complète des propriétés. Ce que vous voyez dépend de la sélection de votre type de carte.

- *network-object*. Cliquez sur la variable et sélectionnez l'objet réseau qui définit l'espace d'adresse que vous souhaitez agréger. L'objet doit utiliser un adressage IPv4 ou IPv6 qui correspond au type d'adresse que vous configurez. Par exemple, vous pouvez agréger les routes pour tous les sous-réseaux 10.0.0.0/8.
- **suppress-map** *carte de route de suppression*. Cliquez sur la variable et sélectionnez la carte de routage qui supprime l'annonce des routes spécifiées. Vous pouvez utiliser les clauses match de la carte de route pour supprimer sélectivement certaines routes plus spécifiques de l'agrégat et en laisser d'autres non supprimées. La carte de route peut faire correspondre les routes en fonction des listes d'accès et des chemins de système autonome.
- **advertise-map** *advertise-route-map*. Cliquez sur la variable et sélectionnez la carte de route qui sélectionne les routes spécifiques qui seront utilisées pour créer différents composants de la route agrégée, telles que AS_SET ou communauté. C'est utile lorsque les composants d'un agrégat se trouvent dans des systèmes autonomes distincts et que vous souhaitez créer un agrégat avec AS_SET et l'annoncer à certains des mêmes systèmes autonomes. Vous devez vous souvenir d'omettre les numéros de système autonome spécifiques de AS_SET pour éviter que l'agrégat soit abandonné par le mécanisme de détection de boucle de BGP sur le routeur de réception. La carte de route peut faire correspondre les routes en fonction des listes d'accès et des chemins de système autonome.
- **attribute-map** *attribute-route-map*. Cliquez sur la variable et sélectionnez la carte de routage qui modifie les attributs de la route agrégée. Cela est utile lorsque l'une des routes composant l'AS_SET est configurée avec un attribut tel que l'attribut de communauté sans exportation, ce qui empêcherait l'exportation de la route agrégée.
- *options*. Cliquez sur la variable et sélectionnez une, toutes ou aucune des options suivantes :
  - **as-set**. Générer des informations de chemin AS_SET pour la route agrégée. Le chemin annoncé pour cette route sera un AS_SET composé de tous les éléments contenus dans tous les chemins en cours de résumé. N'utilisez pas ce mot-clé lors de l'agrégation de nombreux chemins, car cette route doit être continuellement retirée et mise à jour à mesure que les informations de joignabilité des chemins de système autonome changent pour les routes résumées.
  - **summary-only**. Supprimer les annonces de routes plus spécifiques à tous les voisins.

Étape 8 Vous pouvez cliquer sur **...** > **Duplicate (Dupliquer)** à côté de la commande **configure aggregate-address** pour configurer des routes supplémentaires à agréger.

Étape 9 Cliquez sur **OK**.

Configurer les paramètres de filtre de BGP pour IPv4

Vous pouvez créer des règles de filtrage pour restreindre les informations de routage que le système apprend d'autres protocoles de routage ou qu'il leur annonce.

La configuration expliquée ici s'applique à tous les processus locaux et au filtrage des mises à jour de tous les voisins BGP. Vous pouvez configurer différentes règles de filtrage par voisin dans les paramètres de voisin.

Avant de commencer

Créez les objets de liste d'accès standard de l'interface de ligne de commande Smart dont vous avez besoin pour chaque règle de filtre. Utilisez les entrées de contrôle d'accès (ACE) pour filtrer les routages qui correspondent à l'entrée et autorisez les ACE pour les routes qui doivent être mises à jour.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **Routing** (Routage) dans le résumé.

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez le BGP.

Étape 3 Cliquez sur l'onglet **BGP**.

Étape 4 Ajoutez ou modifiez l'objet de processus BGP.

Les commandes de filtrage se trouvent dans les ensembles de commandes sous la commande **configure address family ipv4**. Vous devez configurer la famille d'adresses pour configurer le filtrage. Ces règles ne sont pas disponibles pour IPv6.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) pour exposer toutes les commandes, puis cliquez sur **+** pour activer la commande **configure filter-rules** *direction*.

Étape 6 Cliquez sur *direction* et sélectionnez **in**, pour filtrer les mises à jour entrantes, ou **out**, pour filtrer les mises à jour sortantes.

Étape 7 Pour les filtres entrants, vous pouvez éventuellement spécifier l'interface sur laquelle filtrer les mises à jour. Si vous ne spécifiez pas d'interface, le filtre s'applique à toutes les mises à jour reçues sur n'importe quelle interface.

a) Cliquez sur **+** pour activer la commande **distribute-list** *acl-name* **in** **interface** *interface*.

b) Cliquez sur la variable *interface* et sélectionnez l'interface.

Étape 8 Pour les filtres sortants, vous pouvez éventuellement spécifier le protocole, pour limiter le filtre aux routes annoncées à ce processus de routage.

Il existe deux formes de la commande **distribute-list out**, une avec une variable *d'identifiant* après la variable *de protocole* et l'autre sans l'identifiant. Vous pouvez sélectionner les protocoles suivants, mais ils sont répartis entre ces versions de commande selon que vous devez fournir les informations d'identifiant supplémentaires.

- **connected**. Pour les routes établies pour les réseaux qui sont directement connectés aux interfaces du système.
- **static**. Pour les routes statiques que vous avez créées manuellement.

- **rip**. Pour les routes annoncées à RIP.
- **bgp** *système autonome*. Pour les routes annoncées à BGP. Cliquez sur *l'identifiant* et saisissez le numéro de système autonome pour le processus BGP défini sur le système.
- **eigrp** *système autonome*. Pour les routes annoncées à l'EIGRP. Cliquez sur *l'identifiant* et saisissez le numéro de système autonome pour le processus EIGRP défini sur le système.
- **ospf** *process-id*. Pour les routes annoncées à OSPF. Cliquez sur *l'identifiant* et saisissez l'ID de processus pour le processus OSPF défini sur le système.

Étape 9 Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **configure filter-rules** pour définir une autre règle de filtre. Définissez-en autant que vous le souhaitez.

Étape 10 Cliquez sur **OK**.

Configurer les voisins BGP

Vous devez définir les voisins avec lesquels BGP échangera les mises à jour de routage.

Avant de commencer

Plusieurs commandes facultatives nécessitent des objets Smart CLI, pour les cartes de routage, les listes de préfixes, etc. Examinez les options que vous devez configurer pour déterminer si vous avez besoin d'objets. Vous devez créer les objets Smart CLI avant de configurer la commande BGP associée.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **Routing** (Routage) dans le résumé.

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez le BGP.

Étape 3 Cliquez sur l'onglet **BGP**.

Étape 4 Ajoutez ou modifiez l'objet de processus BGP.

Les commandes voisins se trouvent dans les ensembles de commandes sous la commande **configure address family ipv4** ou **ipv6**. Vous devez configurer les voisins séparément pour chaque famille d'adresses.

Étape 5 Cliquez sur **Show Disabled** (Afficher désactivé) pour exposer toutes les commandes, puis cliquez sur **+** pour activer la commande **configure neighbor**.

Étape 6 Configurez les paramètres de base sur la commande neighbor :

- **neighbor** *neighbor-address*. Cliquez sur la variable et saisissez l'adresse IPv4 ou IPv6 du routeur voisin BGP, selon le cas pour le groupe d'adresses que vous configurez.
- **remote-as** *as-number*. Cliquez sur la variable et saisissez le numéro de système autonome du routeur voisin BGP.
- *config-options*. Cliquez sur la variable et sélectionnez **properties**. La seule propriété configurée par défaut active le voisin. Vous pouvez ajuster d'autres options comme expliqué dans cette procédure.

Étape 7 (Facultatif) Configurer les paramètres généraux du voisin.

a) Cliquez sur **+** pour activer la commande **configure neighbor** *neighbor-address* **remote-as** *settings (paramètres)*. Cliquez sur **Show Disabled** (Afficher désactivé) si vous ne pouvez pas voir la commande.

b) Cliquez sur *Settings* (Paramètres) et sélectionnez **general**.

c) Dans la commande **configure neighbor description**, cliquez sur la variable et saisissez une description du voisin (comme son emplacement ou son objectif), jusqu'à 80 caractères, ou cliquez sur **-** pour désactiver la commande si vous ne souhaitez pas de description. Une description ne peut pas inclure d'espaces ni de points d'interrogation.

d) (IPv4 uniquement.) La commande **configure neighbor shutdown** est initialement activée. Cette commande désactive la communication avec ce voisin BGP, met fin à toute session active et supprime toutes les informations de routage associées. Si vous souhaitez communiquer activement avec ce voisin, cliquez sur **-** pour désactiver cette commande.

e) Pour la commande **configure neighbor fall-over bfd**, cliquez sur *option* et sélectionnez **single-hop** ou **multi-hop** (en fonction de la configuration BFD), ou cliquez sur **-** pour désactiver la commande.

Cette commande enregistre BGP pour recevoir des messages d'échec de détection de chemin de transfert de la part de la détection de transfert bidirectionnel (BFD). Le choix de saut unique ou de saut multiple dépend du type de modèle BFD que vous avez créé et associé à l'interface qui fait face à ce voisin. Assurez-vous que votre sélection ici est conforme au modèle BFD. Vous devez utiliser FlexConfig pour créer et appliquer des modèles BFD.

Étape 8 (Facultatif) Configurer les paramètres avancés du voisin.

a) Si vous l'avez déjà configuré, cliquez sur **...** > **Duplicate** > **(Dupliquer)** pour la commande **configure neighbor** *neighbor-address settings* **remote-as** *de paramètres*, ou simplement cliquez sur le **signe plus (+)** pour l'activer si elle n'est pas encore utilisée. Cliquez sur **Show Disabled** (Afficher désactivé) si vous ne pouvez pas voir la commande.

b) Cliquez sur *Settings* (Paramètres) et sélectionnez **advanced**.

c) Dans la commande **neighbor password**, cliquez sur la variable *secrète* et sélectionnez l'objet de clé secrète qui contient le mot de passe à utiliser lors de l'authentification du voisin, ou cliquez sur **-** pour désactiver la commande si vous ne souhaitez pas utiliser l'authentification du message condensé 5 (MD5). Vous pouvez créer l'objet de clé lors de la modification de l'objet de BGP.

L'objet de clé secrète doit contenir un mot de passe sensible à la casse d'une longueur maximale de 25 caractères. La chaîne peut contenir n'importe quel caractère alphanumérique, y compris des espaces, et les caractères spéciaux ` ~ ! @ # $ % ^ & * () - _ = + | \ } ] { [ " ` : ; / > <., ?. 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.

Assurez-vous que le voisin est configuré pour utiliser le même mot de passe.

d) Dans la commande **configure neighbor hops**, cliquez sur la variable *« options »* et sélectionnez l'une des options suivantes, ou cliquez sur **-** pour désactiver la commande si l'homologue ne se trouve pas à plusieurs sauts (c'est-à-dire s'il n'est pas directement connecté à ce système). Utilisez ces options avec prudence, car vous pouvez vous retrouver avec des boucles de routage et des routes oscillantes : la configuration uniquement des homologues directement connectés est préférable.

- **ebgp-multihop**. Sélectionnez Allow connections with neighbor that is not directly connected (Autoriser les connexions avec un voisin qui n'est pas directement connecté) pour accepter et tenter des connexions BGP avec des homologues externes situés sur des réseaux qui ne sont pas directement connectés. Si vous sélectionnez cette option, les commandes suivantes sont ajoutées :
  - **neighbor ebgp-multihop 255**. Cliquez sur 255, puis saisissez la valeur de durée de vie (TTL) en nombre de sauts, de 1 à 255.

- **neighbor disable-connected-check**. Cliquez sur le signe + pour activer cette commande afin de désactiver la vérification de connexion et établir une session d'homologation eBGP avec un homologue à saut unique utilisant une interface de boucle avec retour. Si l'homologue n'est pas directement connecté au même segment de réseau, la vérification de la connexion empêchera l'établissement de la session d'homologation.

- **ttl-security-hop**. Sécurisez une session d'homologation BGP et configurez le nombre maximal de sauts qui séparent deux homologues BGP externes (eBGP). Si vous sélectionnez cette option, la commande suivante est ajoutée :

  neighbor ttl-security hops *hop-count*. Cliquez sur la variable et saisissez le nombre maximal de sauts qui séparent les homologues, de 1 à 254.

  La commande **neighbor ttl-security** fournit un mécanisme de sécurité allégé pour protéger les sessions d'homologation BGP contre les attaques basées sur l'utilisation du processeur (CPU). Ces types d'attaques sont généralement des attaques de déni de service (DoS) en force brute qui tentent de désactiver le réseau en l'inondant de paquets IP qui contiennent des adresses IP de source et de destination forgées dans les en-têtes de paquet.

  Cette fonctionnalité tire parti du comportement conçu des paquets IP en n'acceptant que les paquets IP dont le nombre de TTL est égal ou supérieur à la valeur configurée localement. La modification précise du nombre de TTL dans un paquet IP est généralement considérée comme impossible. La forge précise d'un paquet pour qu'il corresponde au nombre de TTL d'un homologue de confiance n'est pas possible sans un accès interne au réseau source ou de destination.

  Pour maximiser l'efficacité de cette fonctionnalité, la valeur du nombre de sauts doit être configurée strictement pour correspondre au nombre de sauts entre le réseau local et externe. Cependant, vous devez également prendre en compte la variation de chemin lors de la configuration de cette fonctionnalité pour une session d'homologation multisauts. Assurez-vous de configurer cette fonctionnalité sur tous les routeurs du réseau.

e) Dans la commande **neighbor version**, cliquez sur la variable *de numéro de version* et saisissez 4 pour forcer le logiciel à utiliser BGP version 4, ou cliquez sur **-** pour désactiver la commande. Le logiciel utilise la version 4 par défaut et négocie à la baisse jusqu'à la version 2 de manière dynamique si nécessaire. Configurer la version 4 pour cette commande empêche la négociation de version.

f) Dans la commande **neighbor transport connection-mode**, cliquez sur la variable *options* et sélectionnez si la connexion TCP est **active** ou **passive**, ou cliquez sur **-** pour désactiver la commande et laisser le mode par défaut.

g) Dans la commande **neighbor transport path-mtu-discovery**, cliquez sur la variable *options* et sélectionnez **blank** pour activer la découverte du chemin MTU, ou **disable** pour le désactiver. Sélectionner le champ vide équivaut à cliquer sur **-** pour désactiver la commande, car le système effectue la découverte du chemin MTU par défaut. La découverte du chemin MTU permet à la session BGP de profiter de liens MTU plus importants.

Étape 9 (Facultatif) Configurez les paramètres de migration du voisin.

Les paramètres de migration configurent la commande **neighbor local-as**. La commande **neighbor local-as** est utilisée pour personnaliser l'attribut AS_PATH en ajoutant et en supprimant des numéros de système autonome pour les routes reçues des voisins eBGP. La configuration de cette commande permet à un routeur d'apparaître aux homologues externes en tant que membre d'un autre système autonome aux fins de la migration du numéro de système autonome. Cette fonctionnalité simplifie le processus de modification du numéro de système autonome dans un réseau BGP en permettant à l'opérateur de réseau de migrer les clients vers de nouvelles configurations pendant les périodes de service normales, sans perturber les accords d'homologation existants.

Vous pouvez effectuer cette migration uniquement pour les véritables sessions d'homologation eBGP. Cette commande ne fonctionne pas pour deux homologues dans différents systèmes sous-autonomes d'une confédération.

Mise en garde
BGP fait précéder le numéro de système autonome de chaque réseau BGP qu'une route traverse pour maintenir les informations relatives à la joignabilité du réseau et pour éviter les boucles de routage. Configurez cette commande uniquement pour la migration du système autonome, et désactivez-la une fois la transition achevée. La procédure ne doit être tentée que par un opérateur de réseau expérimenté. Des boucles de routage peuvent être créées par une configuration inadéquate.

a) Si vous l'avez déjà configuré, cliquez sur **...** > **Duplicate** > **(Dupliquer)** pour la commande **configure neighbor** *neighbor-address settings* **remote-as** *de paramètres*, ou simplement cliquez sur le **signe plus (+)** pour l'activer si elle n'est pas encore utilisée. Cliquez sur **Show Disabled** (Afficher désactivé) si vous ne pouvez pas voir la commande.
b) Cliquez sur *Settings* (Paramètres) et sélectionnez **migration**. Cela ajoute la commande suivante :

   configure *neighbor-address* **local-as** *local-as-number options*

c) Cliquez sur la variable *local-as-number* et saisissez le numéro de système autonome local (AS) à ajouter à l'attribut AS_PATH, de 1 à 4294967295 (notation asplain) ou de 1.0 à 65535.65535 (notation asdot). Vous ne pouvez pas spécifier le numéro de système autonome à partir du processus de routage de BGP local ou du réseau de l'homologue distant.
d) Cliquez sur la variable *d'options* et sélectionnez l'une des options suivantes. Notez que la sélection d'un élément dans cette liste (autre que **none**) sélectionne également toutes les options au-dessus dans la liste. C'est normal : les options ne sont pas vraiment indépendantes.

   - **none**. Ne configurez aucune des options suivantes.
   - **no-prepend**. Ne pas ajouter le numéro du système autonome local aux routes reçues du voisin eBGP.
   - **replace-as**. Remplacez le numéro de système autonome réel par le numéro de système autonome local dans les mises à jour d'eBGP. Le numéro de système autonome du processus de routage de BGP local n'est pas ajouté au début.
   - **dual-as**. Configurez le voisin eBGP pour établir une session d'homologation en utilisant le numéro réel du système autonome (du processus de routage BGP local) ou en utilisant le numéro du système autonome local.

Étape 10 (Facultatif. IPv4 uniquement.) Configurez les paramètres de haute disponibilité (HA) du voisin.

Les paramètres du mode HA configurent la commande **neighbor ha-mode graceful-restart**, qui active ou désactive la capacité de redémarrage progressif pour un voisin BGP individuel. Utilisez le mot-clé de désactivation pour désactiver la capacité de redémarrage progressif lorsque le redémarrage progressif a été précédemment activé pour l'homologue de BGP.

La capacité de redémarrage progressif est négociée entre les homologues compatibles avec le transfert sans arrêt (NSF) et NSF dans les messages OUVERTS lors de l'établissement de la session. Si vous activez la capacité de redémarrage progressif après l'établissement d'une session de BGP, vous devrez redémarrer la session avec une réinitialisation logicielle ou matérielle.

Le paramètre en mode HA configure le redémarrage progressif pour un voisin individuel. Au lieu de cela, vous pouvez utiliser les paramètres globaux de BGP pour activer le redémarrage progressif pour tous les voisins.

a) Si vous l'avez déjà configuré, cliquez sur **...** > **Duplicate** > **(Dupliquer)** pour la commande **configure neighbor** *neighbor-address settings* **remote-as** *de paramètres*, ou simplement cliquez sur le **signe plus (+)** pour l'activer si elle n'est pas encore utilisée. Cliquez sur **Show Disabled** (Afficher désactivé) si vous ne pouvez pas voir la commande.
b) Cliquez sur *Settings* (Paramètres) et sélectionnez **ha-mode**.
c) Si vous souhaitez désactiver le redémarrage progressif, cliquez sur *options* de la commande **neighbor ha-mode graceful-restart** et sélectionnez **disable**. Sélectionnez vide pour inverser une action de désactivation précédente.

Étape 11 (Facultatif) Configurez les options d'activation des voisins.

Lorsque vous configurez un nouveau voisin, il est activé par défaut. Vous devez activer les paramètres d'activation si vous souhaitez que le voisin soit désactivé au départ ou configurer d'autres paramètres d'activation.

a) Cliquez sur **+** pour activer la commande **configure neighbor** *neighbor-address* **activate** *activate-options*. Cliquez sur **Show Disabled** (Afficher désactivé) si vous ne pouvez pas voir la commande.
b) Cliquez sur *activate-options* et sélectionnez **properties**.
c) La commande **neighbor** *neighbor-address* **activate** est ajoutée à l'état activé. Cliquez sur **-** pour désactiver la commande et configurer le voisin comme initialement désactivé. Vous devrez modifier cet objet pour activer le voisin lorsque vous serez prêt à communiquer avec lui.

Étape 12 (Facultatif) Configurez le filtrage dans les paramètres d'activation de voisin.

a) Si vous l'avez déjà configuré, cliquez sur **...** > **Duplicate** > **(Dupliquer)** pour la commande **configure neighbor** *neighbor-address settings* **activate** *de paramètres*, ou simplement cliquez sur le **signe plus (+)** pour l'activer si elle n'est pas encore utilisée. Cliquez sur **Show Disabled** (Afficher désactivé) si vous ne pouvez pas voir la commande.
b) Cliquez sur *Settings* (Paramètres) et sélectionnez **filtering**.
c) Configurez le filtrage pour contrôler les préfixes reçus ou envoyés à ce voisin à l'aide de n'importe quelle combinaison des commandes de voisin suivantes. Cliquez sur **-** pour désactiver ceux que vous ne souhaitez pas utiliser. Toutes ces commandes permettent le filtrage dans les sens entrant et sortant : cliquez sur **...** > **Duplicate** > **(Dupliquer)** pour une commande si vous souhaitez configurer les deux sens.

   N'appliquez pas à la fois une commande **neighbor distribute-list** et **neighbor prefix-list** à un voisin dans la même direction. Ces deux commandes s'excluent mutuellement et une seule d'entre elles peut être appliquée à chaque direction entrante ou sortante.

   - **distribute-list** *acl options*. (IPv4 uniquement.) Filtrez les préfixes en fonction de la liste d'accès standard (ACL) sélectionnée. Ensuite, cliquez sur *Options* et choisissez d'appliquer le filtre dans les sens **in** ou **out**.
   - **route-map** *route-map options*. Filtrez les préfixes en fonction de la carte de routage sélectionnée. Ensuite, cliquez sur *Options* et choisissez d'appliquer le filtre dans les sens **in** ou **out**. Dans la carte de routage, vous pouvez configurer le filtrage en fonction de la liste d'accès, du chemin AS, du préfixe et des listes de distribution.
   - **prefix-list** *prefix-list options*. Filtrer les préfixes en fonction de la liste de préfixes IPv4 ou IPv6 sélectionnée. Ensuite, cliquez sur *Options* et choisissez d'appliquer le filtre dans les sens **in** ou **out**.
   - **filter-list** *as-path options*. Filtrer les préfixes en fonction de l'objet filtre AS Path sélectionné. Ensuite, cliquez sur *Options* et choisissez d'appliquer le filtre dans les sens **in** ou **out**.

d) Dans la commande **configure prefix-limit neighbor** *neighbor-address limit-options*, cliquez sur *limit-options*, puis sélectionnez l'une des options suivantes, ou cliquez sur **-** pour désactiver la commande.

La sélection d'une option ajoute une forme de la commande **neighbor maximum-prefix**, avec des options supplémentaires que vous devez configurer. Utilisez cette commande pour contrôler le nombre de préfixes qui peuvent être reçus du voisin.

- **none**. Configurez la forme de base de la commande sans paramètres supplémentaires. Cliquez sur les variables et configurez les valeurs suivantes :
  - max-prefix-limit. Le nombre maximal de préfixes autorisés pour ce voisin, de 1 à 2 147 483 647. Vous devez également configurer cette variable si vous sélectionnez l'une des autres options.
  - **75** (seuil). Le pourcentage du maximum à partir duquel le routeur commence à générer un message d'avertissement, de 1 à 100. La valeur par défaut est 75 %.
- **restart**. Arrêtez la session d'homologation avec le voisin lorsque la limite est atteinte. Cliquez sur la variable *restart-interval* et configurez la durée d'attente du système avant de redémarrer la session, de 1 à 65 535 minutes.
- **warning-only**. N'arrêtez pas la session lorsque la limite est atteinte. Au lieu de cela, envoyez simplement un message syslog d'avertissement et poursuivez la session.

Étape 13 (Facultatif) Configurez les routes dans les paramètres d'activation du voisin.

a) Si vous l'avez déjà configuré, cliquez sur **...** > **Duplicate** > **(Dupliquer)** pour la commande **configure neighbor** *neighbor-address settings* **activate** *de paramètres*, ou simplement cliquez sur le **signe plus (+)** pour l'activer si elle n'est pas encore utilisée. Cliquez sur **Show Disabled** (Afficher désactivé) si vous ne pouvez pas voir la commande.

b) Cliquez sur *Settings* (Paramètres) et sélectionnez **routes**.

c) Dans la commande **neighbor advertisement-interval**, cliquez sur la variable *de valeur* et saisissez l'intervalle minimal d'annonce de route entre l'envoi des mises à jour de route à ce voisin, de 0 à 600 secondes, ou cliquez sur **-** pour désactiver la commande et laisser l'intervalle par défaut à 0, pour iBGP et pour les sessions eBGP dans un routeur virtuel ou 30 pour les sessions eBGP qui ne sont pas dans un routeur virtuel. La valeur 0 signifie que le système enverra des mises à jour chaque fois que la table de routage changera, quelle que soit la fréquence.

d) Dans la commande **neighbor advertise-map**, configurez les options suivantes pour annoncer sous condition les routes sélectionnées au voisin, ou cliquez sur **-** pour désactiver la commande, en envoyant ainsi toutes les mises à jour de route au voisin sans condition.

   Les routes (préfixes) qui seront annoncées sous condition sont définies dans deux cartes de routage : une carte d'annonce et une carte existante ou une carte non existante.

   La carte de routage associée à la carte existante ou à la carte non existante spécifie le préfixe que le locuteur BGP suivra.

   La carte de routage associée à la carte d'annonce spécifie le préfixe qui sera annoncé au voisin précisé lorsque la condition est remplie.

   Lors de la configuration d'une exist map, la condition est remplie lorsque le préfixe existe dans Advertise Map et Exist Map.

   Lors de la configuration d'une Non-exist Map, la condition est remplie lorsque le préfixe existe dans Advertise Map, mais n'existe pas dans Non-exist Map.

   Si la condition n'est pas remplie, la route est retirée et l'annonce conditionnelle ne se produit pas. Toutes les routes qui peuvent être annoncées dynamiquement ou non annoncées doivent exister dans la table de routage de BGP pour que l'annonce conditionnelle se produise.

- *advertise-route-map*. Cliquez sur cette variable et sélectionnez la carte de routage qui définit les routes à annoncer si les conditions de la carte existante ou de la carte inexistante sont remplies.
- *options condition-route-map*. Cliquez sur option et sélectionnez l'une des options suivantes :
  - **exist-map**. Cliquez sur la variable et sélectionnez la carte de routage existante.
  - **non-exist-map**. Cliquez sur la variable et sélectionnez la carte de routage inexistante.

e) La commande **neighbor** *adresse de voisin* **remove-private-as** est ajoutée à l'état activé. Cliquez sur le signe moins (–) pour désactiver la commande. Cette commande supprime les numéros de système autonome privé des mises à jour de routage sortant eBGP. Les valeurs du système autonome privé sont comprises entre 64512 et 65535.

f) Dans la commande **configure neighbor default-originate**, cliquez sur *options* et sélectionnez l'une des options suivantes, ou cliquez sur - pour désactiver la commande.

- **none**. Permet au système d'envoyer une voie de routage par défaut au voisin sans condition.
- **route-map**. Demandez au système d'envoyer sous condition une route par défaut au voisin. Lorsqu'elle est utilisée avec une carte de routage, la route par défaut est injectée si la carte de routage contient une clause d'adresse IP correspondante et qu'il existe une route qui correspond exactement à la liste d'accès IP. Vous pouvez utiliser des listes d'accès standard ou étendues dans la carte de routage pour définir les routes par défaut. Vous devez cliquer sur la variable *route-map* dans la commande **neighbor default-originate** ajoutée à l'objet et sélectionner la carte de routage.

Étape 14 (Facultatif) Configurez les minuteurs dans les paramètres d'activation du voisin.

Si vous configurez des minuteurs pour un voisin, les paramètres remplacent les minuteurs configurés pour tous les voisins BGP dans les paramètres BGP globaux.

a) Si vous l'avez déjà configuré, cliquez sur **...** > **Duplicate** > **(Dupliquer)** pour la commande **configure neighbor** *neighbor-address settings* **activate** *de paramètres*, ou simplement cliquez sur le **signe plus (+)** pour l'activer si elle n'est pas encore utilisée. Cliquez sur **Show Disabled** (Afficher désactivé) si vous ne pouvez pas voir la commande.

b) Cliquez sur *Settings* (Paramètres) et sélectionnez **timers**.

c) Dans la commande **neighbors timers**, configurez les variables suivantes :

- *keepalive-interval*. La fréquence à laquelle le système envoie des messages keepalive à ce voisin, de 0 à 65 535 secondes. La valeur par défaut est de 60 secondes si vous ne configurez pas cette commande.
- *hold-time*. L'intervalle après lequel, en l'absence de message keepalive, le système déclare ce voisin inactif, de 0 à 65 535 secondes. La valeur par défaut est de 180 secondes si vous ne configurez pas cette commande.
- **0** (délai de rétention minimal). Le délai de rétention minimal acceptable qui peut être configuré sur ce voisin, de 0 à 65 535 secondes. Cette valeur doit être inférieure ou égale au délai de rétention configuré pour ce système. Si le délai de rétention du voisin est inférieur à cette valeur, le système n'établira pas de session de BGP avec le voisin.

Étape 15 (Facultatif) Configurez les paramètres d'activation avancée des voisins.

a) Si vous l'avez déjà configuré, cliquez sur **...** > **Duplicate** > **(Dupliquer)** pour la commande **configure neighbor** *neighbor-address settings* **activate** *de paramètres*, ou simplement cliquez sur le **signe plus**

(+) pour l'activer si elle n'est pas encore utilisée. Cliquez sur **Show Disabled** (Afficher désactivé) si vous ne pouvez pas voir la commande.

b) Cliquez sur *Settings* (Paramètres) et sélectionnez **advanced**.

c) Décidez laquelle des commandes **neighbor** suivantes laisser activée. Cliquez sur **-** pour désactiver les options indésirables.

- **send-community**. Envoyer l'attribut de la communauté à ce voisin.
- **weight** *value (valeur)*. Cliquez sur la variable pour attribuer le poids initial aux routes apprises de ce voisin, de 0 à 65 535. Si vous ne configurez pas cette commande, les routes apprises d'un autre homologue de BGP ont un poids par défaut de 0 et les routes provenant du routeur local ont un poids par défaut de 32 768. Cependant, tout poids de route défini à l'aide d'une carte de routage remplace le poids configuré à l'aide de cette commande.
- **next-hop-self**. Configurez le routeur comme prochain saut pour un voisin BGP. Cette commande est utile dans les réseaux non maillés (comme le relayage de trames ou X.25) où les voisins BGP peuvent ne pas avoir d'accès direct à tous les autres voisins sur le même sous-réseau IP.

Étape 16 Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **configure neighbor** pour définir un autre voisin. Définissez-en autant que vous le souhaitez.

Étape 17 Cliquez sur **OK**.

Configurer la redistribution du routage BGP à partir d'autres protocoles de routage

Vous pouvez contrôler la redistribution des routes dans un processus BGP à partir d'autres protocoles de routage, des routes connectées et des routes statiques.

Avant de commencer

Il est conseillé de configurer le processus de routage à partir duquel vous redistribuerez les routes et de déployer vos modifications avant de configurer la redistribution dans BGP.

Si vous souhaitez appliquer une carte de routage pour affiner les routes redistribuées, créez l'objet de carte de routage Smart CLI. Les routes qui correspondent à la carte de routage sont redistribuées, et toutes les routes qui ne correspondent pas ne sont pas redistribuées.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur **Routing** (Routage) dans le résumé.

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez le BGP.

Étape 3 Cliquez sur l'onglet **BGP**.

Étape 4 Ajoutez ou modifiez l'objet de processus BGP.

Les commandes de redistribution se trouvent dans les ensembles de commandes sous la commande **configure address family ipv4** ou **ipv6**. Vous devez configurer la famille d'adresses pour configurer la redistribution.

Étape 5 Cliquez sur **Show Disabled** (Afficher les éléments désactivés) pour exposer toutes les commandes, puis cliquez sur **+** pour activer la commande **configure ipv4/ipv6 redistribution**.

Étape 6 Cliquez sur la variable *protocol* (protocole) et sélectionnez le processus source à partir duquel vous redistribuez les routes. Vous pouvez redistribuer les routes **connected** et **static**, ou les routes générées par **eigrp** (IPv4 uniquement), **isis**, **ospf** ou **rip** (IPv4 uniquement).

Étape 7 Si vous sélectionnez un processus de routage, cliquez sur la variable *identifier* (identifiant) et saisissez la valeur requise :

- **eigrp**. Saisissez le numéro du système autonome.
- **ospf**. Saisissez le numéro d'ID de processus.
- **connected**, **static**, **isis**, **rip**. Entrez **none**. Même si vous saisissez une valeur différente, elle sera ignorée.

Étape 8 (Facultatif ; IS-IS uniquement.) Dans la commande **redistribute isis level-2**, cliquez sur **level-2** et sélectionnez si vous redistribuez les routes apprises uniquement dans une zone IS-IS (**level-1**), entre les zones IS-IS (**level-2**) ou les deux (**level-1-2**).

Étape 9 (Facultatif ; tous les protocoles.) Pour affiner les mesures pour les routes redistribuées, cliquez sur **+** pour activer la commande suivante et configurer les options :

redistribute *valeur métrique* **metric** *du protocole*

Cliquez sur la variable et saisissez la valeur de mesure pour les routes en cours de distribution, de 0 à 4294967295.

Étape 10 (Facultatif ; tous les protocoles.) Pour affiner les routes redistribuées en fonction d'une carte de routage, cliquez sur **+** pour activer la commande **redistribute route-map**, cliquez sur la variable et sélectionnez la carte de routage qui définit vos restrictions.

Si vous n'appliquez pas de carte de routage, toutes les routes du processus (qui correspondent aux autres commandes configurées pour la redistribution) sont redistribuées.

Étape 11 (Facultatif ; OSPF uniquement.) Les commandes suivantes sont activées par défaut lorsque vous redistribuez les routes d'un protocole OSPF. Vous pouvez cliquer sur **-** pour désactiver les commandes indésirables.

Ces commandes précisent les critères selon lesquels les routes OSPF sont redistribuées dans d'autres domaines de routage.

- **redistribute ospf match external 1**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 1.
- **redistribute ospf match external 2**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 2.
- **redistribute ospf match internal**. Routes internes à un système autonome spécifique.
- **redistribute ospf match nssa-external 1**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 1 et marquées comme Not-So-Stubby-Area (NSSA) uniquement.
- **redistribute ospf match nssa-external 2**. Routes externes au système autonome, mais importées dans OSPF en tant que routes externes de type 2 et marquées comme Not-So-Stubby-Area (NSSA) uniquement.

Étape 12 Vous pouvez cliquer sur **...** > **Duplicate** > **(Dupliquer)** à côté de la commande **configure redistribution** pour configurer la redistribution pour un autre protocole. Configurez la redistribution pour chaque protocole qui a du sens pour votre réseau.

Étape 13 Cliquez sur **OK**.

Supervision BGP

Pour surveiller et dépanner BGP, ouvrez la console de l'interface de ligne de commande ou connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes. Vous pouvez également sélectionner certaines de ces commandes dans le menu **Commands (Commandes)** sur la page Routing (Routage).

Utilisez **show bgp ?** pour obtenir des listes d'options supplémentaires. Par exemple, vous pouvez préciser le numéro de système autonome et le routeur virtuel pour limiter les informations que vous voyez, ainsi que d'autres options pour cibler uniquement les informations que vous recherchez. La liste suivante n'est qu'un résumé.

- **show bgp**

  Affiche le contenu du tableau de routage BGP.

- **show bgp cidr-only**

  Affiche les routes avec des masques de réseau non naturels (c'est-à-dire, routage interdomaine sans classe ou CIDR).

- **show bgp community**

  Affiche les routes qui appartiennent à des communautés de BGP spécifiées.

- **show bgp community-list**

  Affiche les routes autorisées par la liste de communautés BGP.

- **show bgp filter-list** *access-list-number*

  Affiche les routes conformes à une liste de filtres spécifiée.

- **show bgp injected-paths**

  Affiche tous les chemins injectés dans la table de routage BGP.

- **show bgp ipv4 unicast**

  Affiche les entrées de la table de routage BGP IP version 4 (IPv4) pour les sessions de monodiffusion.

- **show bgp ipv6 unicast**

  Affiche les entrées de la table de routage BGP IPv6.

- **show bgp neighbors**

  Affiche des renseignements sur les connexions BGP et TCP à des voisins.

- **show bgp paths**

  Affiche tous les chemins de données BGP dans la base de données.

- **show bgp prefix-list**

  Affiche les informations sur une liste de préfixes ou les entrées de liste de préfixes.

- **show bgp regexp** *regexp*

  Affiche les routes qui correspondent à l'expression régulière du chemin du système autonome.

- **show bgp rib-failure**

  Affiche les routes BGP dont l'installation a échoué dans le tableau RIB (Routing Information Base).

- **show bgp summary**

  Affiche l'état de toutes les connexions BGP.

- **show bgp update-group**

  Affiche les renseignements sur les groupes de mise à jour de BGP.



PARTIE V

Politiques de sécurité

- Déchiffrement SSL, à la page 449
- Stratégies d'identité, à la page 475
- Renseignements de sécurité, à la page 491
- Contrôle d'accès, à la page 497
- Stratégies de prévention des intrusions , à la page 539
- Traduction d'adresses réseau (NAT), à la page 565



CHAPITRE 18

Déchiffrement SSL

Certains protocoles, comme HTTPS, utilisent Secure Sockets Layer (SSL) ou son successeur, Transport Layer Security (TLS), pour chiffrer le trafic en vue d'une transmission sécurisée. Comme le système ne peut pas inspecter les connexions chiffrées, vous devez les déchiffrer si vous souhaitez appliquer des règles d'accès qui tiennent compte des caractéristiques de trafic de couche supérieure pour prendre des décisions en matière d'accès.

- À propos du déchiffrement SSL, à la page 449
- Exigences de licence pour le déchiffrement SSL, à la page 453
- Lignes directrices pour l'utilisation du déchiffrement, à la page 453
- Comment mettre en œuvre et maintenir la politique de déchiffrement SSL, à la page 454
- Configuration des politiques de déchiffrement SSL, à la page 456
- Exemple : blocage des anciennes versions SSL/TLS du réseau, à la page 470
- Surveillance et dépannage du déchiffrement SSL, à la page 472

À propos du déchiffrement SSL

Normalement, les connexions passent par la politique de contrôle d'accès pour déterminer si elles sont autorisées ou bloquées. Toutefois, si vous activez la politique de déchiffrement SSL, les connexions chiffrées sont d'abord envoyées par l'intermédiaire de la politique de déchiffrement SSL pour déterminer si elles doivent être déchiffrées ou bloquées. Toute connexion qui n'a pas été bloquée, qu'elle soit déchiffrée ou non, est ensuite soumise à la politique de contrôle d'accès pour une décision finale d'autorisation ou de blocage.

Remarque Vous devez activer la politique de déchiffrement SSL pour mettre en œuvre les règles d'authentification active dans la politique d'identité. Si vous activez le déchiffrement SSL pour activer les politiques d'identité, mais que vous ne souhaitez pas autrement mettre en œuvre le déchiffrement SSL, sélectionnez Do Not Decrypt (Ne pas déchiffrer) pour l'action par défaut et ne créez pas de règles de déchiffrement SSL supplémentaires. La politique d'identité génère automatiquement les règles dont elle a besoin.

Les rubriques suivantes expliquent plus en détail la gestion et le déchiffrement du flux de trafic chiffré.

Pourquoi mettre en œuvre le déchiffrement SSL?

Le trafic chiffré, comme les connexions HTTPS, ne peut pas être inspecté.

De nombreuses connexions sont légitimement chiffrées, notamment les connexions aux banques et à d'autres établissements financiers. De nombreux sites Web utilisent le chiffrement pour protéger la confidentialité ou les données sensibles. Par exemple, votre connexion au FDM est chiffrée.

Cependant, les utilisateurs peuvent également masquer le trafic indésirable dans les connexions chiffrées.

En mettant en œuvre le déchiffrement SSL, vous pouvez déchiffrer les connexions, les inspecter pour vérifier qu'elles ne contiennent pas de menaces ou d'autre trafic indésirable, puis les chiffrer à nouveau avant de poursuivre la connexion. (Le trafic déchiffré passe par votre politique de contrôle d'accès et correspond aux règles en fonction des caractéristiques inspectées de la connexion déchiffrée, et non des caractéristiques chiffrées.) Cela équilibre votre besoin d'appliquer des politiques de contrôle d'accès avec le besoin de l'utilisateur de protéger les informations sensibles.

Vous pouvez également configurer des règles de déchiffrement SSL pour bloquer le trafic chiffré des types que vous savez ne pas vouloir sur votre réseau.

Gardez à l'esprit que le déchiffrement puis le rechiffrement du trafic ajoute une charge de traitement sur le périphérique, ce qui réduira les performances globales du système.

Actions que vous pouvez appliquer au trafic chiffré

Lors de la configuration des règles de déchiffrement SSL, vous pouvez appliquer les actions décrites dans les rubriques suivantes. Ces actions sont également disponibles pour l'action par défaut, qui s'applique à tout trafic qui ne correspond pas à une règle explicite.



Remarque Tout trafic qui passe par la politique de déchiffrement SSL doit ensuite passer par la stratégie de contrôle d'accès. À l'exception du trafic que vous abandonnez dans la politique de déchiffrement SSL, la décision finale d'autorisation ou d'abandon dépend de la stratégie de contrôle d'accès.

Déchiffrer - Resigner

Si vous choisissez de déchiffrer et de signer le trafic de nouveau, le système agit comme un intermédiaire.

Par exemple, l'utilisateur saisit https://www.cisco.com dans un navigateur. Le trafic atteint le périphérique Firepower Threat Defense, le périphérique négocie ensuite avec l'utilisateur à l'aide du certificat d'autorité de certification spécifié dans la règle et crée un tunnel SSL entre l'utilisateur et le périphérique Firepower Threat Defense. En même temps, le périphérique se connecte à https://www.cisco.com et crée un tunnel SSL entre le serveur et le périphérique Firepower Threat Defense.

Ainsi, le client voit le certificat de l'autorité de certification configuré pour la règle de déchiffrement SSL au lieu du certificat de www.cisco.com. Le client doit faire confiance au certificat pour terminer la connexion. Le périphérique Firepower Threat Defense effectue ensuite le déchiffrement/rechiffrement dans les deux sens du trafic entre le client et le serveur de destination.



Remarque Si le client ne fait pas confiance à l'autorité de certification (CA) utilisée pour signer de nouveau le certificat du serveur, il avertit l'utilisateur que le certificat ne doit pas être approuvé. Pour éviter cela, importez le certificat d'autorité de certification dans le magasin d'autorités de certification de confiance du client. Sinon, si votre entreprise dispose d'une PKI privée, vous pouvez émettre un certificat d'autorité de certification intermédiaire signé par l'autorité de certification racine et qui est automatiquement approuvé par tous les clients de l'organisation, puis téléverser ce certificat d'autorité de certification sur le périphérique.

Si vous configurez une règle avec l'action Decrypt Re-Sign (Déchiffrer et resigner), la règle correspond au trafic en fonction du type d'algorithme de signature du certificat interne de l'autorité de certification référencé, en plus des conditions de la règle configurée. Comme vous pouvez sélectionner un seul certificat de resignature pour la politique de déchiffrement SSL, cela peut limiter le trafic correspondant pour les règles de resignature.

Par exemple, le trafic sortant chiffré à l'aide d'un algorithme de courbe elliptique (EC) correspond à une règle Déchiffrer - Resigner uniquement si le certificat de resignature est un certificat d'autorité de certification basé sur EC. De même, une règle Decrypt Re-Sign (Déchiffrer et resigner) qui fait référence à un certificat d'autorité de certification basé sur RSA correspond uniquement au trafic sortant chiffré avec un algorithme RSA; le trafic sortant chiffré avec un algorithme EC ne correspond pas à la règle, même si toutes les autres conditions de règle configurées correspondent.

Déchiffrer à l'aide d'une clé connue

Si vous êtes propriétaire du serveur de destination, vous pouvez mettre en œuvre le déchiffrement avec une clé connue. Dans ce cas, lorsque l'utilisateur ouvre une connexion à https://www.cisco.com, l'utilisateur voit le certificat réel pour www.cisco.com, même si c'est le périphérique Firepower Threat Defense qui présente le certificat.



Votre entreprise doit être le propriétaire du domaine et du certificat. Pour l'exemple de cisco.com, la seule façon possible de faire en sorte que l'utilisateur final voie le certificat de Cisco serait si vous êtes propriétaire du domaine cisco.com (c'est-à-dire que vous êtes Cisco Systems) et que vous êtes propriétaire du certificat cisco.com signé par une autorité de certification publique (CA). Vous ne pouvez déchiffrer qu'avec des clés connues pour les sites appartenant à votre organisation.

L'objectif principal du déchiffrement avec une clé connue est de déchiffrer le trafic dirigé vers votre serveur HTTPS pour protéger vos serveurs contre les attaques externes. Pour inspecter le trafic côté client vers des

sites HTTPS externes, vous devez utiliser la re-signature du déchiffrement, car vous n'êtes pas propriétaire des serveurs.

Remarque Pour utiliser le déchiffrement par clé connue, vous devez charger le certificat et la clé du serveur en tant que certificat d'identité interne, puis l'ajouter à la liste des certificats de clé connue dans les paramètres de la politique de déchiffrement SSL. Vous pouvez ensuite écrire la règle de déchiffrement par clé connue en utilisant l'adresse du serveur comme adresse de destination. Pour en savoir plus sur l'ajout du certificat à la politique de déchiffrement SSL, consultez Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement, à la page 467.

Ne pas déchiffrer

Si vous choisissez de contourner le déchiffrement pour certains types de trafic, aucun traitement n'est effectué sur le trafic. Le trafic chiffré est dirigé vers la stratégie de contrôle d'accès, où il est autorisé ou abandonné en fonction de la règle de contrôle d'accès à laquelle il correspond.

Bloquer

Vous pouvez simplement bloquer le trafic chiffré qui correspond à une règle de déchiffrement SSL. Le blocage dans la politique de déchiffrement SSL empêche la connexion d'atteindre la politique de contrôle d'accès.

Lorsque vous bloquez une connexion HTTPS, l'utilisateur ne voit pas la page de réponse de blocage par défaut du système. Au lieu de cela, l'utilisateur voit la page par défaut du navigateur pour un échec de connexion sécurisée. Le message d'erreur n'indique pas que le site a été bloqué en raison de la politique. Au lieu de cela, des erreurs peuvent indiquer qu'il n'y a pas d'algorithmes de chiffrement communs. Ce message n'indique pas clairement que la connexion a été bloquée intentionnellement.

Règles de déchiffrement SSL générées automatiquement

Que vous activiez ou non la politique de déchiffrement SSL, le système génère automatiquement des règles de re-signature de déchiffrement pour chaque règle de politique d'identité qui met en œuvre l'authentification active. Cela est nécessaire pour activer l'authentification active pour les connexions HTTPS.

Lorsque vous activez la politique de déchiffrement SSL, ces règles s'affichent sous l'en-tête Règles d'authentification actives de la politique d'identité. Ces règles sont regroupées en haut de la politique de déchiffrement SSL. Les règles sont en lecture seule. Vous pouvez les modifier uniquement en modifiant votre politique d'identité.

Gestion du trafic non déchiffrable

Plusieurs caractéristiques rendent une connexion indéchiffrable. Si une connexion possède l'une des caractéristiques suivantes, l'action par défaut est appliquée à la connexion, quelle que soit la règle à laquelle la connexion correspondrait. Si vous sélectionnez Bloquer comme action par défaut (plutôt que Ne pas déchiffrer), vous pourriez rencontrer des problèmes, notamment des pertes excessives de trafic légitime.

- Session compressée : une compression de données a été appliquée à la connexion.
- Session SSLv2 : la version minimale de SSL prise en charge est SSLv3.

- Unknown cipher suite (suite de chiffrement inconnu) : le système ne reconnaît pas la suite de chiffrement pour la connexion.
- Unsupported cipher suite : le système ne prend pas en charge le déchiffrement selon la suite de chiffrement détectée.
- Session not cached (session non mise en cache) : la session SSL a la réutilisation de session activée, le client et le serveur ont rétabli la session avec l'identifiant de session et le système n'a pas mis en cache cet identifiant de session.
- Handshake errors (Erreurs d'établissement de liaison) : une erreur s'est produite lors de la négociation d'établissement de liaison SSL.
- Decryption error (erreurs de déchiffrement) : une erreur s'est produite lors de l'opération de déchiffrement.
- Passive interface traffic (trafic d'interface passive) : tout le trafic sur les interfaces passives (zones de sécurité passives) est non déchiffrable.

Exigences de licence pour le déchiffrement SSL

Vous n'avez pas besoin de licence particulière pour utiliser la politique de déchiffrement SSL.

Cependant, vous avez besoin de la licence **URL** pour créer des règles qui utilisent les catégories et la réputation d'URL comme critères de correspondance. Pour en savoir plus sur la configuration des licences, consultez Activation ou désactivation des licences facultatives, à la page 95.

Lignes directrices pour l'utilisation du déchiffrement

Gardez les éléments suivants à l'esprit lors de la configuration et de la surveillance des politiques de déchiffrement SSL :

- La politique de déchiffrement SSL est contournée pour toutes les connexions qui correspondent aux règles de contrôle d'accès avec des actions Trust (Confiance), Block (Blocage) ou Block with reset (Blocage avec réinitialisation) si ces règles :
  - Utilisez la zone de sécurité, le réseau, la géolocalisation et le port uniquement comme critères de correspondance de trafic.
  - précède d'autres règles qui nécessitent une inspection, telles que les règles qui font correspondre les connexions en fonction de l'application ou de l'URL, ou les règles d'autorisation qui appliquent l'inspection des intrusions ou des fichiers.
- Lors de l'utilisation de la mise en correspondance de catégorie d'URL, notez qu'il existe des cas où la page de connexion d'un site se trouve dans une catégorie différente de celle du site lui-même. Par exemple, Gmail se trouve dans la catégorie « Courriels sur le Web », alors que la page de connexion se trouve dans la catégorie « Portails Internet ». Pour faire déchiffrer les connexions à ces sites, vous devez inclure les deux catégories dans la règle.
- Si une mise à jour de la base de données des vulnérabilités (VDB) supprime (abandonne) les applications, vous devez apporter des modifications aux règles de déchiffrement SSL ou aux filtres d'application qui utilisent l'application supprimée. Vous ne pouvez pas déployer les modifications avant d'avoir corrigé ces règles. En outre, vous ne pouvez pas installer les mises à jour du logiciel système avant de résoudre

le problème. Dans la page d'objet des filtres d'application ou dans l'onglet Application de la règle, ces applications indiquent « (Deprecated) » (Obsolète) après le nom de l'application.

- Vous ne pouvez pas désactiver la politique de déchiffrement SSL si vous avez des règles d'authentification actives. Pour désactiver la politique de déchiffrement SSL, vous devez soit désactiver la politique d'identité, soit supprimer toutes les règles d'identité qui utilisent l'authentification active.

Comment mettre en œuvre et maintenir la politique de déchiffrement SSL

Vous pouvez utiliser les politiques de déchiffrement SSL pour convertir le trafic chiffré en trafic de texte brut, afin de pouvoir ensuite appliquer le filtrage d'URL, la prévention des intrusions et des programmes malveillants, ainsi que d'autres services nécessitant une inspection approfondie des paquets. Si vos politiques le permettent, le trafic est rechiffré avant de quitter le périphérique.

La politique de déchiffrement SSL s'applique uniquement au trafic chiffré. Aucune connexion non chiffrée n'est évaluée par rapport aux règles de déchiffrement SSL.

Contrairement à certaines autres politiques de sécurité, vous devez surveiller et maintenir activement la politique de déchiffrement SSL, car les certificats peuvent expirer ou même être modifiés sur les serveurs de destination. En outre, les modifications apportées au logiciel client peuvent altérer votre capacité à déchiffrer certaines connexions, car l'action de re-signer le déchiffrement est impossible à distinguer d'une attaque de type Man-in-the-middle (d'intermédiaire).

La procédure suivante explique le processus de bout en bout de mise en œuvre et de maintenance de la politique de déchiffrement SSL.

Procédure

Étape 1 Si vous mettez en œuvre les règles de déchiffrement et de réauthentification, créez le certificat d'autorité de certification interne requis.

Vous devez utiliser un certificat d'autorité de certification (CA) interne. Vous avez les options suivantes. Étant donné que les utilisateurs doivent faire confiance au certificat, téléversez soit un certificat déjà approuvé par les navigateurs clients, soit assurez-vous que le certificat téléversé est ajouté aux magasins de certificats de confiance des navigateurs.

- Créez un certificat d'autorité de certification interne autosigné, qui est signé par le périphérique lui-même. Consultez Génération de certificats internes autosignés et de certificats d'autorité de certification internes, à la page 163.
- Chargez un certificat d'autorité de certification interne et une clé signée par une autorité de certification externe de confiance ou par une autorité de certification de votre organisation. Consultez Charger les certificats d'identité interne et d'autorité de certification interne, à la page 161.

Étape 2 Si vous mettez en œuvre les règles de déchiffrement de la clé connue, collectez le certificat et la clé sur chacun des serveurs internes.

Vous ne pouvez utiliser le déchiffrement de la clé connue qu'avec les serveurs que vous contrôlez, car vous devez obtenir le certificat et la clé du serveur. Chargez ces certificats et clés en tant que certificats internes

(et non en tant que certificats d'autorité de certification interne). Consultez Charger les certificats d'identité interne et d'autorité de certification interne, à la page 161.

Étape 3 Activer la politique de déchiffrement SSL., à la page 457.

Lorsque vous activez la politique, vous configurez également certains paramètres de base.

Étape 4 Configurer l'action de déchiffrement SSL par défaut, à la page 459.

En cas de doute, sélectionnez **Do Not Decrypt (Ne pas déchiffrer)** comme action par défaut. Votre stratégie de contrôle d'accès peut tout de même abandonner le trafic qui correspond à la règle de déchiffrement SSL par défaut, au besoin.

Étape 5 Configurer les règles de déchiffrement SSL, à la page 459.

Déterminez le trafic à déchiffrer et le type de déchiffrement à appliquer.

Étape 6 Si vous configurez le déchiffrement par clé connue, modifiez les paramètres de la politique de déchiffrement SSL pour inclure ces certificats. Consultez Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement, à la page 467.

Étape 7 Si nécessaire, téléchargez le certificat d'autorité de certification utilisé pour les règles de déchiffrement et de réauthentification et chargez-le dans le navigateur sur les postes de travail clients.

Pour en savoir plus sur le téléchargement du certificat et sa distribution aux clients, consultez Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature, à la page 469.

Étape 8 Périodiquement, mettez à jour les certificats de réauthentification et de clé connue.

- Certificat de réauthentification : mettez à jour ce certificat avant son expiration. Si vous générez le certificat par le biais de Gestionnaire de périphériques de pare-feu, il est valide pendant 5 ans. Pour vérifier la période de validité d'un certificat, sélectionnez **Objects (Objets)** > **Certificates (Certificats)**, repérez le certificat dans la liste, puis cliquez sur l'icône d'information () correspondante dans la colonne Actions. La boîte de dialogue d'information affiche la période de validité et certaines autres caractéristiques. Vous pouvez également téléverser un certificat de remplacement à partir de cette page.
- Certificat de clé connue : pour toute règle de déchiffrement de clé connue, vous devez vous assurer d'avoir chargé le certificat et la clé actuels du serveur de destination. Chaque fois que le certificat et la clé changent sur les serveurs pris en charge, vous devez également charger le nouveau certificat et la clé (en tant que certificat interne) et mettre à jour les paramètres de déchiffrement SSL pour utiliser le nouveau certificat.

Étape 9 Chargez les certificats d'autorité de certification de confiance manquants pour les serveurs externes.

Le système comprend un large éventail de certificats racine d'autorité de certification et intermédiaires de confiance émis par des tiers. Ceux-ci sont nécessaires lors de la négociation de la connexion entre leFirepower Threat Defense et les serveurs de destination pour les règles de déchiffrement et de réauthentification.

Chargez tous les certificats de la chaîne de confiance d'une autorité de certification racine dans la liste des certificats d'autorités de certification de confiance, y compris le certificat de l'autorité de certification racine et tous les certificats d'autorités de certification intermédiaires. Sinon, il est plus difficile de détecter les certificats de confiance émis par des autorités de certification intermédiaires. Chargez les certificats sur la page **Objects (Objets)** > **Certificates (Certificats)**. Consultez Téléchargement des certificats de l'autorité de certification de confiance, à la page 165.

Configuration des politiques de déchiffrement SSL

Vous pouvez utiliser les politiques de déchiffrement SSL pour convertir le trafic chiffré en trafic de texte brut, afin de pouvoir ensuite appliquer le filtrage d'URL, la prévention des intrusions et des programmes malveillants, ainsi que d'autres services nécessitant une inspection approfondie des paquets. Si vos politiques le permettent, le trafic est rechiffré avant de quitter le périphérique.

La politique de déchiffrement SSL s'applique uniquement au trafic chiffré. Aucune connexion non chiffrée n'est évaluée par rapport aux règles de déchiffrement SSL.

Remarque Les tunnels VPN sont déchiffrés avant l'évaluation de la politique de déchiffrement SSL, de sorte que la politique ne s'applique jamais au tunnel lui-même. Cependant, toute connexion chiffrée dans le tunnel est soumise à une évaluation par la politique de déchiffrement SSL.

La procédure suivante explique comment configurer la politique de déchiffrement SSL. Pour une explication du processus de bout en bout de création et de gestion du déchiffrement SSL, voir Comment mettre en œuvre et maintenir la politique de déchiffrement SSL, à la page 454.

Avant de commencer

Le tableau des règles de déchiffrement SSL contient deux sections :

- **Règles d'authentification active de la politique d'identité** : si vous activez la politique d'identité et créez des règles qui utilisent l'authentification active, le système crée automatiquement les règles de déchiffrement SSL nécessaires pour faire fonctionner ces politiques. Ces règles sont toujours évaluées avant les règles de déchiffrement SSL que vous créez vous-même. Vous ne pouvez modifier ces règles qu'indirectement, en modifiant la politique d'identité.
- **Règles natives SSL** : il s'agit de règles que vous avez configurées. Vous ne pouvez ajouter de règles qu'à cette section.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Si vous n'avez pas encore activé la politique, cliquez sur **Enable SSL Decryption** (Activer le déchiffrement SSL) et configurez les paramètres de la politique, comme décrit dans Activer la politique de déchiffrement SSL., à la page 457.

Étape 2 Configurez l'action par défaut pour la politique.

Le choix le plus sûr est **Do Not Decrypt** (Ne pas déchiffrer). Pour en savoir plus, consultez Configurer l'action de déchiffrement SSL par défaut, à la page 459.

Étape 3 Gérez la politique de déchiffrement SSL.

Après avoir configuré les paramètres de déchiffrement SSL, cette page répertorie toutes les règles dans l'ordre. Les règles sont comparées au trafic du haut vers le bas, la première correspondance détermine l'action à appliquer. Vous pouvez effectuer ce qui suit à partir de cette page :

- Pour désactiver la politique, cliquez sur le bouton de bascule **SSL Decryption Policy** (politique de déchiffrement SSL). Vous pouvez la réactiver en cliquant sur **Enable SSL Decryption** (Activer le déchiffrement SSL).
- Pour modifier les paramètres de la politique, y compris la liste des certificats utilisés dans la politique, cliquez sur le bouton **SSL Decryption Settings** (Paramètres de déchiffrement SSL) (). Vous pouvez également télécharger le certificat utilisé avec les règles de reconnexion de déchiffrement afin de pouvoir le distribuer aux clients. Consultez les rubriques suivantes:
  - Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement, à la page 467
  - Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature, à la page 469
- Pour configurer des règles :
  - Pour créer une nouvelle règle, cliquez sur le bouton +. Consultez Configurer les règles de déchiffrement SSL, à la page 459.
  - Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle (dans la colonne Actions). Vous pouvez également modifier de manière sélective une propriété de règle en cliquant sur la propriété dans le tableau.
  - Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression () de la règle (dans la colonne Actions).
- Pour déplacer une règle, modifiez-la et sélectionnez le nouvel emplacement dans la liste déroulante **Order** (Ordre).
- Si des règles rencontrent des problèmes, par exemple en raison de catégories d'URL supprimées ou modifiées, cliquez sur le lien **See Problem Rules** (voir les règles pour lesquelles il y a des problèmes) à côté de la zone de recherche pour filtrer le tableau afin d'afficher uniquement ces règles. Veuillez modifier et corriger (ou supprimer) ces règles afin qu'elles fournissent le service dont vous avez besoin.

Activer la politique de déchiffrement SSL.

Avant de pouvoir configurer les règles de déchiffrement SSL, vous devez activer la politique et configurer certains paramètres de base. La procédure suivante explique comment activer la politique directement. Vous pouvez également l'activer lorsque vous activez les politiques d'identité. Les politiques d'identité nécessitent que vous activiez la politique de déchiffrement SSL.

Avant de commencer

Si vous avez effectué la mise à niveau à partir d'une version qui n'avait pas de politiques de déchiffrement SSL, mais que vous aviez configuré la politique d'identité avec des règles d'authentification actives, la politique de déchiffrement SSL est déjà activée. Assurez-vous de sélectionner le certificat de déchiffrement Re-Sign que vous souhaitez utiliser et activez éventuellement les règles prédéfinies.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Étape 2 Cliquez sur **Enable SSL Decryption** (activer le déchiffrement SSL) pour configurer les paramètres de la politique.

- S'il s'agit de la première fois que vous avez activé la politique, la boîte de dialogue SSL Decryption Configuration (Configuration du déchiffrement SSL) s'ouvre. Passez à l'étape suivante.
- Si vous avez déjà configuré la politique une fois, puis l'avez désactivée, la politique est simplement réactivée avec vos paramètres et règles précédents. Vous pouvez cliquer sur le bouton **SSL Decryption Settings** (Paramètres de déchiffrement SSL) () et configurer les paramètres comme décrit dans Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement, à la page 467.

Étape 3 Dans **Decrypt Re-Sign Certificate** (Déchiffrer le certificat re-signé), sélectionnez le certificat d'autorité de certification interne à utiliser pour les règles mettant en œuvre le déchiffrement avec des certificats re-signés.

Vous pouvez utiliser le certificat NGFW-Default-InternalCA prédéfini ou celui que vous avez créé ou téléversé. Si le certificat n'existe pas encore, cliquez sur **Create Internal CA** (créer une autorité de certification interne) pour le créer.

Si vous n'avez pas encore installé le certificat dans les navigateurs clients, cliquez sur le bouton de téléchargement () pour en obtenir une copie. Consultez la documentation de chaque navigateur afin de savoir comment installer le certificat. Voir aussi Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature, à la page 469.

Étape 4 (Facultatif) Cliquez sur le signe **plus (+)** sous **Trusted CA Certificates** (Certificats d'autorité de certification approuvés) et sélectionnez les certificats ou les groupes de certificats auxquels vous souhaitez que la politique fasse confiance.

Le groupe par défaut, Cisco-Trusted-Authorities, comprend tous les certificats d'autorité de certification de confiance définis par le système. Si vous avez chargé des certificats supplémentaires, vous pouvez les ajouter ici ou les collecter dans votre propre groupe et sélectionner le groupe ici. Vous pouvez soit remplacer le groupe Cisco-Trusted-Authorities, soit simplement ajouter votre groupe. Les utilisateurs seront invités à accepter le certificat pour tout site dont l'autorité de signature du certificat n'est pas représentée dans cette liste : l'accès au site n'est pas bloqué simplement parce que le certificat n'est pas fiable.

Si vous laissez la liste vide ou ne sélectionnez que des groupes de certificats vides, la politique de déchiffrement SSL fera confiance à n'importe quel certificat.

Étape 5 Sélectionnez les règles de déchiffrement SSL initiales.

Le système comprend la règle prédéfinie suivante que vous pourriez trouver utile :

- **Sensitive_Data** (Données_sensibles) : cette règle ne déchiffre pas le trafic qui correspond aux sites Web dans les catégories d'URL Services financiers ou d'URL de santé et de médecine, qui comprennent les banques, les services de santé, etc. Vous devez activer la licence d'URL pour mettre en œuvre cette règle.

Étape 6 Cliquez sur **Enable** (activer).

Configurer l'action de déchiffrement SSL par défaut

Si une connexion chiffrée ne correspond pas à une règle de déchiffrement SSL spécifique, elle est gérée par l'action par défaut de la politique de déchiffrement SSL.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Étape 2 Cliquez n'importe où dans le champ **Default Action** (action par défaut).

Étape 3 Sélectionnez l'action à appliquer au trafic correspondant.

- **Do Not Decrypt** (Ne pas déchiffrer) : autorise la connexion chiffrée. La stratégie de contrôle d'accès évalue ensuite la connexion chiffrée et l'abandonne ou l'autorise en fonction des règles de contrôle d'accès.
- **Block** (Bloquer) : interrompt la connexion immédiatement. La connexion n'est pas transmise à la stratégie de contrôle d'accès.

Étape 4 (Facultatif) Configurez la journalisation pour l'action par défaut.

Vous devez activer la journalisation du trafic correspondant à la règle pour qu'elle soit incluse dans les données du tableau de bord ou le visualisateur d'événements. Sélectionnez parmi les options suivantes :

- **At End of Connection** (À la fin de la connexion) : génère un événement à la fin de la connexion.
  - **Send Connection Events To** (Envoyer les événements de connexion à) : si vous souhaitez envoyer une copie des événements à un serveur syslog externe, sélectionnez l'objet serveur qui définit le serveur syslog. Si l'objet requis n'existe pas déjà, cliquez sur **Create New Syslog Server** (Créer un nouveau serveur syslog) et créez-le. (Pour désactiver la journalisation sur un serveur syslog, sélectionnez **Any** (N'importe lequel) dans la liste des serveurs.)

    Comme le stockage d'événements sur l'appareil est limité, l'envoi des événements à un serveur journal système externe peut fournir un stockage à plus long terme et améliorer votre analyse des événements.
- **No Logging** (Aucune journalisation) : ne génère aucun événement.

Étape 5 Cliquez sur **Save** (Enregistrer).

Configurer les règles de déchiffrement SSL

Utilisez les règles de déchiffrement SSL pour déterminer comment gérer les connexions chiffrées. Les règles de la politique de déchiffrement SSL sont évaluées de haut en bas. La règle appliquée au trafic est la première s'appliquant, entraînant la mise en correspondance de tous les critères de trafic.

Vous pouvez créer et modifier des règles uniquement dans la section SSL Native Rules (Règles SSL natives).

Remarque Le trafic pour vos connexions VPN (de site à site et d'accès à distance) est déchiffré avant que la politique de déchiffrement SSL n'évalue les connexions. Ainsi, les règles de déchiffrement SSL ne sont jamais appliquées aux connexions VPN, et vous n'avez pas besoin de prendre en compte les connexions VPN lors de la création de ces règles. Cependant, toute utilisation de connexions chiffrées dans un tunnel VPN est évaluée. Par exemple, une connexion HTTPS à un serveur interne par l'intermédiaire d'une connexion VPN d'accès à distance est évaluée par les règles de déchiffrement SSL, même si le tunnel VPN d'accès à distance lui-même ne l'est pas (car il est déjà déchiffré).

Avant de commencer

Si vous créez une règle de déchiffrement de clé connue, veillez à charger le certificat et la clé pour le serveur de destination (en tant que certificat interne) et à modifier les paramètres de la politique de déchiffrement SSL pour utiliser le certificat. Les règles de clé connue précisent généralement le serveur de destination dans les critères de réseau de destination de la règle. Pour en savoir plus, consultez Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement, à la page 467.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Si vous n'avez configuré aucune règle de déchiffrement SSL (hormis celles générées automatiquement pour les règles d'identité d'authentification actives), vous pouvez ajouter des règles prédéfinies en cliquant sur **Add Pre-Defined Rules** (Ajouter des règles prédéfinies). Vous êtes invité à sélectionner les règles que vous souhaitez.

Étape 2 Effectuez l'une des actions suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle.

Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression ( ) de la règle.

Étape 3 Sous **Order**, sélectionnez l'endroit où vous souhaitez insérer la règle dans la liste ordonnée des règles.

Vous ne pouvez insérer des règles que dans la section **SSL Native Rules** (Règles SSL natives). Les Identity Policy Active Authentication Rules (Règles d'authentification active de la politique d'identité) sont automatiquement générées à partir de votre politique d'identité et sont en lecture seule.

Les règles sont appliquées sur la base de la première correspondance, vous devez donc vous assurer que les règles comprenant des critères de correspondance de trafic très spécifiques apparaissent au-dessus des politiques qui ont des critères plus généraux, qui s'appliqueraient autrement au trafic correspondant.

La valeur par défaut consiste à ajouter la règle à la fin de la liste. Si vous souhaitez modifier l'emplacement d'une règle ultérieurement, modifiez cette option.

Étape 4 Dans **Title** (titre), entrez un nom pour la règle.

Le nom ne peut pas contenir d'espaces. Vous pouvez utiliser des caractères alphanumériques et les caractères spéciaux suivants : + . _ -

Étape 5 Sélectionnez l'action à appliquer au trafic correspondant.

Pour une description détaillée de chaque option, consultez les éléments suivants :

- Déchiffrer - Resigner, à la page 450
- Déchiffrer à l'aide d'une clé connue, à la page 451
- Ne pas déchiffrer, à la page 452
- Bloquer, à la page 452

Étape 6 Définissez les critères de correspondance du trafic en utilisant n'importe quelle combinaison des onglets suivants :

- **Source/Destination** : les zones de sécurité (interfaces) par lesquelles passe le trafic, les adresses IP ou le pays ou le continent (emplacement géographique) de l'adresse IP, ou les ports TCP utilisés dans le trafic. La valeur par défaut est toute zone, adresse, emplacement géographique et port TCP. Consultez Critères de source/destination pour les règles de déchiffrement SSL, à la page 462.
- **Application** : l'application ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. La valeur par défaut est n'importe quelle application chiffrée. Consultez Critères d'application pour les règles de déchiffrement SSL, à la page 463.
- **URL** : la catégorie d'URL d'une requête Web. Par défaut, la catégorie d'URL et la réputation ne sont pas prises en compte à des fins de correspondance. Consultez Critères d'URL pour les règles de déchiffrement SSL, à la page 464.
- **Users** (Utilisateurs) : la source d'identité, l'utilisateur ou le groupe d'utilisateurs. Vos politiques d'identité déterminent si les informations d'utilisateur et de groupe sont disponibles pour la correspondance du trafic. Vous devez configurer les politiques d'identité pour utiliser ce critère. Consultez Critères d'utilisateur pour les règles de déchiffrement SSL, à la page 465.
- **Advanced** (Avancé) : caractéristiques dérivées des certificats utilisés dans la connexion, telles que la version SSL/TLS et l'état du certificat. Consultez Critères avancés pour les règles de déchiffrement SSL, à la page 466.

Pour modifier une condition, vous cliquez sur le bouton **+** dans cette condition, sélectionnez l'objet ou l'élément souhaité, puis cliquez sur **OK** dans la boîte de dialogue contextuelle. Si le critère requiert un objet, vous pouvez cliquer sur **Create New *Object*** (créer un nouvel objet) si l'objet requis n'existe pas. Cliquez sur le **x** d'un objet ou d'un élément pour le supprimer de la politique.

Lorsque vous ajoutez des conditions aux règles de déchiffrement SSL, tenez compte des conseils suivants :

- Vous pouvez configurer plusieurs conditions par règle. Le trafic doit correspondre à toutes les conditions de la règle pour que celle-ci s'applique au trafic. Par exemple, vous pouvez utiliser une règle unique pour déchiffrer le trafic en fonction de la catégorie d'URL.
- Pour chaque condition d'une règle, vous pouvez ajouter jusqu'à 50 critères. Le trafic qui correspond à l'un des critères d'une condition satisfait à la condition. Par exemple, vous pouvez utiliser une règle unique pour appliquer le contrôle d'application à 50 applications ou filtres d'application. Ainsi, il existe une relation OU entre les éléments d'une condition unique, mais une relation ET entre les types de condition (par exemple, entre la source ou destination et l'application).
- La mise en correspondance de la catégorie d'URL nécessite la licence de filtrage d'URL.

Étape 7 (Facultatif) Configurez la journalisation pour la règle.

Vous devez activer la journalisation du trafic correspondant à la règle pour qu'elle soit incluse dans les données du tableau de bord ou le visualisateur d'événements. Sélectionnez parmi les options suivantes :

- **At End of Connection** (À la fin de la connexion) : génère un événement à la fin de la connexion.
  - **Send Connection Events To** (Envoyer les événements de connexion à) : si vous souhaitez envoyer une copie des événements à un serveur syslog externe, sélectionnez l'objet serveur qui définit le serveur syslog. Si l'objet requis n'existe pas déjà, cliquez sur **Create New Syslog Server** (Créer un nouveau serveur syslog) et créez-le. (Pour désactiver la journalisation sur un serveur syslog, sélectionnez Any (N'importe lequel) dans la liste des serveurs.)

    Comme le stockage d'événements sur l'appareil est limité, l'envoi des événements à un serveur journal système externe peut fournir un stockage à plus long terme et améliorer votre analyse des événements.

- **No Logging** (Aucune journalisation) : ne génère aucun événement.

Étape 8 Cliquez sur **OK**.

Critères de source/destination pour les règles de déchiffrement SSL

Les critères Source/Destination d'une règle de déchiffrement SSL définissent les zones de sécurité (interfaces) par lesquelles passe le trafic, les adresses IP ou le pays ou le continent (emplacement géographique) pour l'adresse IP, ou les ports TCP utilisés dans le trafic. La valeur par défaut englobe toute zone, adresse, emplacement géographique et tout port TCP. TCP est le seul protocole correspondant aux règles de déchiffrement SSL.

Pour modifier une condition, vous cliquez sur le bouton **+** dans cette condition, sélectionnez l'objet ou l'élément souhaité, puis cliquez sur **OK**. Si le critère requiert un objet, vous pouvez cliquer sur **Create New *Object*** (créer un nouvel objet) si l'objet requis n'existe pas. Cliquez sur le **x** d'un objet ou d'un élément pour le supprimer de la politique.

Vous pouvez utiliser les critères suivants pour identifier la source et la destination à mettre en correspondance dans la règle.

Zones source, zones de destination

Les objets de la zone de sécurité qui définissent les interfaces par lesquelles passe le trafic. Vous pouvez définir un critère, les deux critères ou aucun critère : tout critère non spécifié s'applique au trafic sur n'importe quelle interface.

- Pour faire correspondre le trafic sortant de l'appareil depuis une interface dans la zone, ajoutez cette zone aux **zones de destination**.
- Pour faire correspondre le trafic entrant dans l'appareil depuis une interface dans la zone, ajoutez cette zone aux zones source (**Source Zones**).
- Si vous ajoutez des conditions de zone source et de zone de destination à une règle, le trafic correspondant doit provenir de l'une des zones source spécifiées et sortir par l'une des zones de destination.

Utilisez ces critères lorsque la règle doit être appliquée en fonction de l'entrée ou de la sortie du trafic sur l'appareil. Par exemple, si vous voulez vous assurer que tout le trafic allant des hôtes externes vers les hôtes internes est déchiffré, vous devez sélectionner votre zone externe comme **Source Zones** (Zones source) et votre zone interne comme **Destination Zones** (Zones de destination).

Réseaux sources, réseaux de destination

Les objets réseau ou les emplacements géographiques qui définissent les adresses réseau ou les emplacements du trafic.

- Pour faire correspondre le trafic d'une adresse IP ou d'un emplacement géographique, configurez les réseaux sources (**Source Networks**).
- Pour faire correspondre le trafic à une adresse IP ou à un emplacement géographique, configurez les réseaux de destination (**Source Networks**).
- Si vous ajoutez des conditions de réseau source et de destination à une règle, le trafic correspondant doit provenir de l'une des adresses IP spécifiées et être destiné à l'une des adresses IP de destination.

Lorsque vous ajoutez ce critère, vous sélectionnez les onglets suivants :

- **Network** (réseau) : Sélectionnez les objets ou groupes réseau qui définissent les adresses IP source ou de destination du trafic que vous souhaitez contrôler.



Remarque Pour les règles de déchiffrement de clé connue, sélectionnez un objet avec l'adresse IP du serveur de destination qui utilise le certificat et la clé que vous avez chargés.

- **Geolocation** (géolocalisation) : Sélectionnez l'emplacement géographique pour contrôler le trafic en fonction de son pays ou continent de source ou de destination. La sélection d'un continent sélectionne tous les pays du continent. En plus de sélectionner l'emplacement géographique directement dans la règle, vous pouvez également sélectionner un objet de géolocalisation que vous avez créé pour définir l'emplacement. En utilisant la localisation géographique, vous pouvez facilement restreindre l'accès à un pays en particulier sans avoir besoin de connaître toutes les adresses IP potentielles qui y sont utilisées.

Ports source, ports/protocoles de destination

Les objets de port qui définissent les protocoles utilisés dans le trafic. Vous pouvez spécifier le protocole TCP et les ports uniquement pour les règles de déchiffrement SSL.

- Pour faire correspondre le trafic d'un port TCP, configurez les **Source Ports** (Ports source).
- Pour faire correspondre le trafic à un port TCP, configurez les **Destination Ports/Protocols** (Ports/Protocoles de destination).
- Pour faire correspondre le trafic provenant de ports TCP spécifiques et destiné à des ports TCP spécifiques, configurez les deux. Par exemple, vous pouvez cibler le trafic du port TCP/80 au port TCP/8080.

Critères d'application pour les règles de déchiffrement SSL

Les critères d'application d'une règle de déchiffrement SSL définissent l'application utilisée dans une connexion IP, ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. La valeur par défaut est toute application qui a la balise SSL Protocol. Vous ne pouvez pas faire correspondre les règles de déchiffrement SSL à une application non chiffrée.

Bien que vous puissiez spécifier des applications individuelles dans la règle, les filtres d'applications simplifient la création et l'administration des politiques. Par exemple, vous pouvez créer une règle de déchiffrement SSL qui déchiffre ou bloque toutes les applications à haut risque et à faible pertinence commerciale. Si un utilisateur tente d'utiliser l'une de ces applications, la session est déchiffrée ou bloquée.

De plus, Cisco met fréquemment à jour et ajoute des détecteurs d'applications supplémentaires par l'intermédiaire des mises à jour du système et de la base de données des vulnérabilités (VDB). Ainsi, une règle pour les applications à risque élevé peut s'appliquer automatiquement aux nouvelles applications sans que vous ayez à mettre à jour la règle manuellement.

Vous pouvez spécifier des applications et des filtres directement dans la règle, ou créer des objets de filtre d'application qui définissent ces caractéristiques. Les spécifications sont équivalentes, bien que l'utilisation d'objets puisse permettre de respecter plus facilement la limite du système de 50 éléments par critère si vous créez une règle complexe.

Pour modifier la liste des applications et des filtres, vous cliquez sur le bouton **+** dans la condition, sélectionnez les applications ou les objets de filtre d'application souhaités, qui sont répertoriés sur des onglets distincts, puis cliquez sur **OK** dans la boîte de dialogue contextuelle. Dans l'un ou l'autre des onglets, vous pouvez cliquer sur **Advanced Filter** (Filtres avancés) pour sélectionner des critères de filtre ou pour vous aider à rechercher des applications spécifiques. Cliquez sur le **x** pour une application, un filtre ou un objet pour le supprimer de la politique. Cliquez sur le lien **Save As Filter** (Enregistrer en tant que filtre) pour enregistrer les critères combinés qui ne sont pas déjà un objet en tant que nouvel objet de filtre d'application.

Pour en savoir plus sur les critères d'application et comment configurer les filtres avancés et sélectionner des applications, consultez Configuration des objets de filtre d'application, à la page 149.

Tenez compte des conseils suivants lors de l'utilisation des critères d'application dans les règles de déchiffrement SSL.

- Le système peut identifier les applications non chiffrées qui deviennent chiffrées à l'aide de StartTLS. Cela inclut des applications telles que SMTPS, POPS, FTPS, TelnetS et IMAPS. En outre, il peut identifier certaines applications chiffrées en fonction de l'indication du nom du serveur dans le message TLS ClientHello ou de la valeur du nom distinctif du sujet provenant du certificat du serveur.
- Le système peut identifier l'application uniquement après l'échange du certificat du serveur. Si le trafic échangé pendant l'établissement de liaison SSL correspond à toutes les autres conditions dans une règle SSL contenant une condition d'application, mais que l'identification n'est pas terminée, la politique SSL permet au paquet de passer. Ce comportement permet à l'établissement de liaison de se faire afin que les applications puissent être identifiées. Une fois que le système a terminé son identification, il applique la règle d'action appropriée au trafic de session restant.
- Si une application sélectionnée a été supprimée par une mise à jour de VDB, « (Deprecated) » s'affiche après le nom de l'application. Vous devez supprimer ces applications du filtre, sinon les déploiements et les mises à niveau logicielles du système suivants seront bloqués.

Critères d'URL pour les règles de déchiffrement SSL

Les critères d'URL d'une règle de déchiffrement SSL définissent la catégorie à laquelle appartient l'URL dans une requête Web. Vous pouvez également préciser la réputation relative des sites à déchiffrer, à bloquer ou à autoriser sans déchiffrement. La valeur par défaut est de ne pas mettre en correspondance les connexions selon les catégories d'URL.

Par exemple, vous pourriez bloquer tous les sites de jeux chiffrés ou déchiffrer les sites de réseaux sociaux non fiables. Si un utilisateur tente d'accéder à une URL avec cette catégorie et ce niveau de réputation, la

session est bloquée ou déchiffrée. Pour en savoir plus sur la mise en correspondance des catégories d'URL, consultez Filtrage des URL par catégorie et par réputation, à la page 503.

Onglet Catégories

Cliquez sur **+**, sélectionnez les catégories souhaitées, puis cliquez sur **OK**. Cliquez sur le **x** pour supprimer une catégorie de la politique.

La valeur par défaut est d'appliquer la règle à toutes les URL de chaque catégorie sélectionnée, quelle que soit leur réputation. Pour limiter la règle en fonction de la réputation, cliquez sur la flèche vers le bas pour chaque catégorie, désélectionnez la case **Any** (Tout), puis utilisez le curseur **Reputation** (Réputation) pour choisir le niveau de réputation. La partie gauche du curseur de réputation indique les sites autorisés sans déchiffrement, tandis que la partie droite regroupe les sites qui seront déchiffrés ou bloqués. La façon dont la réputation est utilisée dépend de l'action de la règle :

- Si la règle déchiffre ou bloque les connexions, la sélection d'un niveau de réputation sélectionne également toutes les réputations plus graves que ce niveau. Par exemple, si vous configurez une règle pour déchiffrer ou bloquer les sites (Suspects) et **Questionable** (Discutables) (niveau 2), elle déchiffre ou bloque également automatiquement les sites (À risque élevé) et **Untrusted** (Non fiables) (niveau 1).
- Si la règle autorise les connexions sans déchiffrement (ne pas déchiffrer), la sélection d'un niveau de réputation sélectionne également toutes les réputations moins graves que ce niveau. Par exemple, si vous configurez une règle pour ne pas déchiffrer les site (Suspects) et **Questionable** (Discutables) (niveau 4), elle ne déchiffre également pas automatiquement les sites (Bien connus) et **Trusted (de confiance)** (niveau 5).

Sélectionnez l'option **Include Sites with Unknown Reputation** (inclure les sites avec une réputation inconnue) pour inclure les URL de réputation inconnue dans la correspondance de réputation. Les nouveaux sites ne sont généralement pas classés, et il peut y avoir d'autres raisons pour lesquelles la réputation d'un site est inconnue ou ne peut être déterminée.

Vérifier la catégorie d'une URL

Vous pouvez vérifier la catégorie et la réputation d'une URL particulière. Saisissez l'URL dans le champ **URL to Check** (URL à vérifier), puis cliquez sur **Go** (Lancer). Vous serez redirigé vers un site Web externe pour consulter les résultats. Si vous êtes en désaccord avec une catégorisation, cliquez sur le lien **Submit a URL Category** Dispute (Soumettre une contestation de catégorie d'URL) et faites-le-nous savoir.

Critères d'utilisateur pour les règles de déchiffrement SSL

Les critères d'utilisateur d'une règle de déchiffrement SSL définissent l'utilisateur ou le groupe d'utilisateurs pour une connexion IP. Vous devez configurer les politiques d'identité et le serveur de répertoire associé pour inclure les critères d'utilisateur ou de groupe d'utilisateurs dans une règle.

Vos politiques d'identité déterminent si l'identité de l'utilisateur est collectée pour une connexion particulière. Si l'identité est établie, l'adresse IP de l'hôte est associée à l'utilisateur identifié. Ainsi, le trafic dont l'adresse IP source est mappée à un utilisateur est considéré comme provenant de cet utilisateur. Les paquets IP en eux-mêmes ne comprennent pas d'informations sur l'identité de l'utilisateur, de sorte que ce mappage adresse IP-utilisateur est la meilleure approximation disponible.

Étant donné que vous pouvez ajouter un maximum de 50 utilisateurs ou groupes à une règle, il est généralement plus logique de sélectionner des groupes que de sélectionner des utilisateurs individuels. Par exemple, vous pouvez créer une règle qui déchiffre le trafic vers le groupe d'ingénierie qui provient du réseau externe, et créer une règle distincte qui ne déchiffre pas le trafic sortant de ce groupe. Ensuite, pour que la règle s'applique

aux nouveaux ingénieurs, il vous suffit d'ajouter le spécialiste en ingénierie au groupe Engineering dans le serveur d'annuaire.

Vous pouvez également sélectionner les sources d'identité à appliquer à tous les utilisateurs de cette source. Ainsi, si vous prenez en charge plusieurs domaines Active Directory, vous pouvez fournir un déchiffrement différentiel en fonction du domaine.

Pour modifier la liste des utilisateurs, vous cliquez sur le bouton **+** dans la condition et sélectionnez les utilisateurs ou les groupes d'utilisateurs souhaités en utilisant l'une des techniques suivantes. Cliquez sur le **x** pour un utilisateur ou un groupe pour le supprimer de la politique.

- **Sources d'identité** : sélectionnez une source d'identité, telle qu'un domaine AD ou la base de données d'utilisateurs locaux, pour appliquer la règle à tous les utilisateurs obtenus à partir des sources sélectionnées. Si le domaine dont vous avez besoin n'existe pas encore, cliquez sur **Create New Identity Realm** (Créer un nouveau domaine d'identité) et créez-le maintenant.
- **Groupes** : sélectionnez les groupes d'utilisateurs souhaités. Les groupes sont disponibles uniquement si vous les configurez dans le serveur de répertoire. Si vous sélectionnez un groupe, la règle s'applique à tous les membres du groupe, y compris les sous-groupes. Si vous souhaitez traiter un sous-groupe différemment, vous devez créer une règle d'accès distincte pour le sous-groupe et la placer au-dessus de la règle pour le groupe parent dans la stratégie de contrôle d'accès.
- **Utilisateurs** : sélectionnez des utilisateurs individuels. Le nom d'utilisateur est précédé de la source d'identité, par exemple Realm\username (domaine\nom_utilisateur).

  Il existe certains utilisateurs intégrés dans le domaine Special-Identities-Realm (domaine d'identités spéciales) :

  - **Failed Authentication** (Échec de l'authentification) : l'utilisateur a été invité à s'authentifier, mais n'a pas réussi à saisir une paire nom d'utilisateur/mot de passe valide dans le nombre maximal de tentatives autorisées. L'échec de l'authentification n'empêche pas l'utilisateur d'accéder au réseau, mais vous pouvez écrire une règle d'accès pour limiter l'accès au réseau pour ces utilisateurs.
  - **Guest** (Invité) : les utilisateurs invités sont similaires aux utilisateurs en Failed Authentication (Échec de l'authentification), sauf que votre règle d'identité est configurée pour identifier ces utilisateurs comme Guest (Invité). Les utilisateurs invités ont été invités à s'authentifier et n'ont pas réussi à le faire dans les limites du nombre maximal de tentatives.
  - **No Authentication Required** (Aucune authentification requise) : l'utilisateur n'a pas été invité à s'authentifier, car ses connexions correspondaient à des règles d'identité ne spécifiant aucune authentification.
  - **Unknown** (Inconnu) : aucun mappage d'utilisateur n'existe pour l'adresse IP et aucun échec d'authentification n'a encore été enregistré. En règle générale, cela signifie qu'aucun trafic HTTP n'a encore été vu à partir de cette adresse.

Critères avancés pour les règles de déchiffrement SSL

Les critères de correspondance de trafic avancé sont liés aux caractéristiques dérivées des certificats utilisés dans la connexion. Vous pouvez configurer les options suivantes :

Options des propriétés du certificat

Le trafic correspond à l'option des propriétés du certificat de la règle s'il correspond à l'une des propriétés sélectionnées. Vous pouvez configurer les éléments suivants :

État du certificat

Si le certificat est **Valid** (valide) ou **Invalid** (non valide). Sélectionnez **Any** (tout) (par défaut) si l'état du certificat n'a pas d'importance.

Un certificat est considéré comme valide si toutes les conditions suivantes sont remplies, sinon il n'est pas valide :

- La politique fait confiance à l'autorité de certification qui a émis le certificat.
- La signature du certificat peut être correctement validée par rapport au contenu du certificat.
- Le certificat de l'autorité de certification émettrice est stocké dans la liste des certificats d'autorités de certification de confiance de la politique.
- Aucune des autorités de certification de confiance de la politique n'a révoqué le certificat.
- La date actuelle est comprise entre la date de début de validité du certificat et la date de fin de validité du certificat.

Autosigné

Le certificat de serveur détecté contient le même nom distinctif d'émetteur et de sujet. Sélectionnez l'une des options suivantes :

- **Self-Signing** (Auto-signature) : le certificat du serveur est autosigné.
- **CA-Signing** (Signature par une autorité de certification) : le certificat du serveur est signé par une autorité de certification. C'est-à-dire que l'émetteur et le sujet ne sont pas la même chose.
- **Any** (Tout) : ne tient pas compte du fait que le certificat est autosigné comme critère de correspondance.

Version prise en charge

La version SSL/TLS à mettre en correspondance. La règle s'applique au trafic qui utilise uniquement les versions sélectionnées. Toutes les versions sont sélectionnées par défaut. Sélectionnez parmi : **SSL 3.0**, **TLS 1.0**, **TLS 1.1**, **TLS 1.2**.

Par exemple, si vous souhaitez autoriser uniquement les connexions TLSv1.2, vous pouvez créer une règle de blocage pour les versions antérieures.

Le trafic qui utilise une version non répertoriée, comme SSL v2.0, est géré par l'action par défaut de la politique de déchiffrement SSL.

Configurer les certificats pour la clé connue et la nouvelle signature du déchiffrement

Si vous mettez en œuvre le déchiffrement, soit par nouvelle signature ou par utilisation de clés connues, vous devez identifier les certificats que les règles de déchiffrement SSL peuvent utiliser. Assurez-vous que tous les certificats sont valides et n'ont pas encore expiré.

Surtout pour le déchiffrement par clé connue, vous devez vous assurer que le système dispose du certificat et de la clé actuels pour chaque serveur de destination dont vous déchiffrez les connexions. Avec une règle de déchiffrement de clé connue, vous utilisez le certificat et la clé réels du serveur de destination pour le déchiffrement. Ainsi, vous devez vous assurer que le périphérique Firepower Threat Defense dispose du certificat et de la clé actuels à tout moment, sinon le déchiffrement échouera.

Chargez un nouveau certificat interne et une nouvelle clé chaque fois que vous modifiez le certificat ou la clé sur le serveur de destination dans une règle de clé connue. Chargez-les en tant que certificat interne (et non en tant que certificat d'autorité de certification interne). Vous pouvez téléverser le certificat au cours de la procédure suivante, ou aller à la page **Objects (Objets)** > **Certificates (Certificats)** et le charger à cet endroit.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Étape 2 Cliquez sur le bouton **SSL Decryption Settings** ( ).

Étape 3 Dans **Decrypt Re-Sign Certificate** (Déchiffrer le certificat re-signé), sélectionnez le certificat d'autorité de certification interne à utiliser pour les règles mettant en œuvre le déchiffrement avec des certificats re-signés.

Vous pouvez utiliser le certificat NGFW-Default-InternalCA prédéfini ou celui que vous avez créé ou téléversé. Si le certificat n'existe pas encore, cliquez sur **Create Internal CA** (créer une autorité de certification interne) pour le créer.

Si vous n'avez pas encore installé le certificat dans les navigateurs clients, cliquez sur le bouton de téléchargement ( ) pour en obtenir une copie. Consultez la documentation de chaque navigateur afin de savoir comment installer le certificat. Voir aussi Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature, à la page 469.

Étape 4 Pour chaque règle qui déchiffre à l'aide d'une clé connue, téléversez le certificat interne et la clé du serveur de destination.

a) Cliquez sur **+** sous **Decrypt Known-Key Certificates** (Déchiffrer les certificats à clé connue).
b) Sélectionnez le certificat d'identité interne ou cliquez sur **Create New Internal Certificate** (créer un nouveau certificat interne) pour le téléverser maintenant.
c) Cliquez sur **OK**.

Étape 5 (Facultatif) Cliquez sur le signe **plus (+)** sous **Trusted CA Certificates** (Certificats d'autorité de certification approuvés) et sélectionnez les certificats ou les groupes de certificats auxquels vous souhaitez que la politique fasse confiance.

Le groupe par défaut, Cisco-Trusted-Authorities, comprend tous les certificats d'autorité de certification de confiance définis par le système. Voici les principaux cas dans lesquels vous pourriez modifier ce paramètre :

- Vous souhaitez utiliser des certificats d'autorité de certification de confiance qui ne sont pas dans le groupe par défaut. Vous devez ensuite sélectionner le groupe par défaut et votre nouveau groupe dans les paramètres de la politique de déchiffrement SSL. Vous pouvez le faire si vous avez chargé des certificats d'autorité de certification de confiance supplémentaires.
- Vous souhaitez utiliser une liste plus limitée de certificats d'autorité de certification de confiance que celle du groupe par défaut. Vous devez ensuite créer un groupe qui a une liste complète de certificats de confiance, pas seulement votre delta, et le sélectionner comme seul groupe dans les paramètres de la politique de déchiffrement SSL.

Les utilisateurs seront invités à accepter le certificat pour tout site dont l'autorité de signature du certificat n'est pas représentée dans cette liste : l'accès au site n'est pas bloqué simplement parce que le certificat n'est pas fiable.

Si vous laissez la liste vide ou ne sélectionnez que des groupes de certificats vides, la politique de déchiffrement SSL fera confiance à n'importe quel certificat.

Étape 6 Cliquez sur **Save** (Enregistrer).

Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature

Si vous décidez de déchiffrer le trafic, les utilisateurs doivent avoir le certificat d'autorité de certification interne qui est utilisé dans le processus de chiffrement défini comme une autorité de certification racine de confiance dans leurs applications utilisant TLS/SSL. Généralement, si vous générez un certificat, ou parfois même si vous en importez un, le certificat n'est pas déjà défini comme un certificat de confiance dans ces applications. Par défaut, dans la plupart des navigateurs Web, lorsque les utilisateurs envoient des requêtes HTTPS, un message d'avertissement de l'application client leur indique qu'il existe un problème avec le certificat de sécurité du site Web. Habituellement, le message d'erreur indique que le certificat de sécurité du site Web n'a pas été émis par une autorité de certification approuvée ou que le site Web a été certifié par une autorité inconnue, mais l'avertissement peut également indiquer qu'il y a une possible attaque de l'homme du milieu en cours. Certaines autres applications client ne présentent pas ce message d'avertissement aux utilisateurs et ne permettent pas aux utilisateurs d'accepter le certificat non reconnu.

Vous disposez des options suivantes pour fournir aux utilisateurs le certificat requis :

Informer les utilisateurs d'accepter le certificat racine

Vous pouvez informer les utilisateurs de votre organisation des nouvelles politiques de l'entreprise et leur dire d'accepter le certificat racine fourni par l'entreprise en tant que source de confiance. Les utilisateurs doivent accepter le certificat et l'enregistrer dans la zone de stockage de l'autorité de certification racine de confiance pour qu'ils ne soient plus invités à le faire lorsqu'ils accèdent au site.



Remarque L'utilisateur doit accepter et faire confiance au certificat d'autorité de certification qui a créé le certificat de remplacement. S'ils font plutôt confiance au certificat du serveur de remplacement, ils continueront à voir des avertissements pour chaque site HTTPS qu'ils visitent.

Ajouter le certificat racine aux périphériques clients

Vous pouvez ajouter le certificat racine à tous les périphériques clients du réseau en tant qu'autorité de certification racine de confiance. De cette façon, les applications client acceptent automatiquement les transactions avec le certificat racine.

Vous pouvez soit rendre le certificat accessible aux utilisateurs en l'envoyant par courriel ou en le plaçant sur un site partagé, soit l'intégrer à l'image de votre poste de travail d'entreprise et utiliser les fonctions de mise à jour de votre application pour le distribuer automatiquement aux utilisateurs.

La procédure suivante explique comment télécharger le certificat d'autorité de certification interne et l'installer sur les clients Windows.

Procédure

Étape 1 Téléchargez le certificat à partir de Gestionnaire de périphériques de pare-feu.

a) Select **Policies (politiques)** > **SSL Decryption**.

b) Cliquez sur le bouton **SSL Decryption Settings** ( ).

c) Cliquez maintenant sur le bouton **Download** pour procédez au téléchargement ( ).

d) Sélectionnez un emplacement de téléchargement, modifiez éventuellement le nom du fichier (mais pas l'extension), puis cliquez sur **Save** (enregistrer).

Vous pouvez maintenant annuler la boîte de dialogue SSL Decryption Settings (paramètres de déchiffrement SSL).

Étape 2 Installez le certificat dans la zone de stockage de l'autorité de certification racine de confiance dans les navigateurs Web sur les systèmes clients, ou mettez-le à la disposition des clients pour qu'ils l'installent eux-mêmes.

Le processus varie selon le système d'exploitation et le type de navigateur. Par exemple, vous pouvez utiliser le processus suivant pour Internet Explorer et Chrome fonctionnant sous Windows. (Pour Firefox, faites l'installation dans la page **Tools (outils)** > **Options (options)** > **Advanced (avancées)**.)

a) Dans le menu **Start** (démarrer), sélectionnez **Control Panel (panneau de configuration)** > **Internet Options (options Internet)**.

b) Sélectionnez l'onglet **Content** (contenu).

c) Cliquez sur le bouton **Certificates** pour ouvrir la boîte de dialogue des certificats.

d) Sélectionnez l'onglet **Trusted Root Certificate Authorities** (autorités de certification racine de confiance).

e) Cliquez sur **Import** (importer), puis suivez l'assistant pour localiser et sélectionner le fichier téléchargé (<uuid> _internalCA.crt) et ajoutez-le au magasin des autorités de certification racine de confiance (Trusted Root Certificate Authorities).

f) Cliquez sur **Finish** (Terminer).

Les messages doivent indiquer que l'importation a réussi. Vous pourriez voir une boîte de dialogue intermédiaire vous avertir que Windows ne pourrait pas valider le certificat si vous avez généré un certificat autosigné plutôt que de l'obtenir auprès d'une autorité de certification tierce bien connue.

Vous pouvez maintenant fermer les boîtes de dialogue Certificate et Internet Options.

Exemple : blocage des anciennes versions SSL/TLS du réseau

Certaines entreprises sont tenues d'empêcher l'utilisation d'anciennes versions de SSL ou de TLS en raison de la réglementation gouvernementale ou de la politique de l'entreprise. Vous pouvez utiliser la politique de déchiffrement SSL pour bloquer le trafic qui utilise une version SSL/TLS que vous interdisez. Il est conseillé de placer cette règle en haut de la politique de déchiffrement SSL pour vous assurer de détecter immédiatement le trafic interdit.

L'exemple suivant bloque toutes les connexions SSL 3.0 et TLS 1.0.

Avant de commencer

Cette procédure suppose que vous ayez déjà activé la politique de déchiffrement SSL, comme expliqué dans la section Activer la politique de déchiffrement SSL., à la page 457.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)**.

Étape 2 Cliquez sur le bouton + pour créer une nouvelle règle.

Étape 3 Dans Order (Ordre), sélectionnez **1** pour placer la règle en haut de la politique, ou sélectionnez le numéro le plus adapté à votre réseau.

La valeur par défaut consiste à ajouter la règle à la fin de la politique.

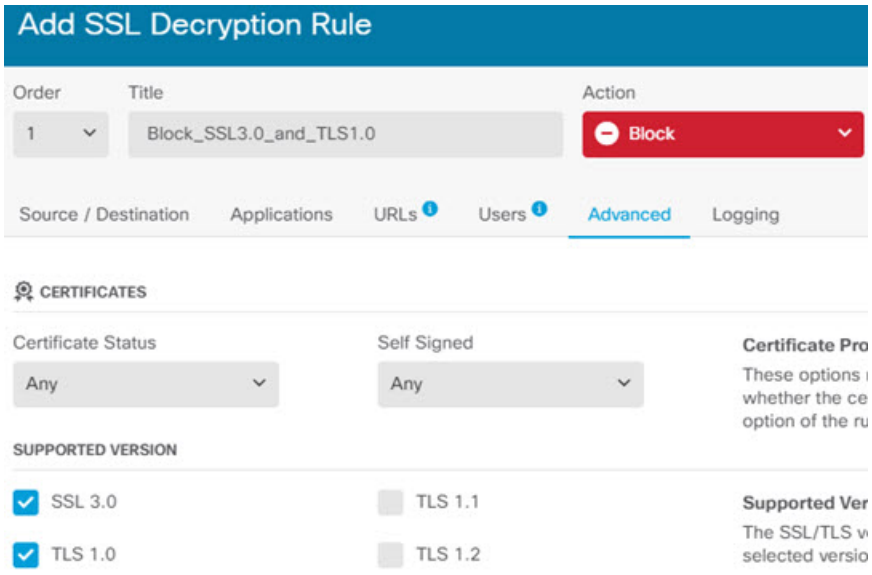
Étape 4 Dans **Title (Titre)**, saisissez un nom pour la règle, par exemple, Block_SSL3.0_and_TLS1.0.

Étape 5 Dans **Action**, sélectionnez **Block** (Bloquer). Cela abandonnera immédiatement tout trafic qui correspond à la règle.

Étape 6 Laissez les valeurs par défaut pour toutes les options sous les onglets suivants : **Source/Destination**, **Applications**, **URLs**, **Users** (utilisateurs).

Étape 7 Cliquez sur l'onglet **Advanced** (Avancé) et sous **Supported Versions** (Versions prises en charge), laissez SSL 3.0 et TLS 1.0 sélectionnés, mais décochez TLS 1.1, TLS 1.2.

La politique doit ressembler à ce qui suit :



Étape 8 (Facultatif) Cliquez sur l'onglet **Logging** (Journalisation) et sélectionnez **At End of Connection** (Événements de fin de connexion) si vous souhaitez que les tableaux de bord et les événements reflètent les connexions bloquées. Vous pouvez également sélectionner un serveur syslog externe si vous en utilisez un.

Étape 9 Cliquez sur **OK**.

Vous pouvez maintenant déployer la politique. Une fois déployée, toute connexion SSL 3.0 ou TLS 1.0 qui passe par le système sera abandonnée.

Remarque

Les connexions SSL 2.0 sont gérées par l'action par défaut pour la politique. Si vous souhaitez vous assurer qu'elles sont également abandonnées, modifiez l'action par défaut pour Block (Bloquer).

Prochaine étape

Si vous mettez en œuvre cette règle, nous avons les recommandations suivantes :

- Pour tout type de règle de déchiffrement, laissez les paramètres par défaut sous l'onglet Advanced (Avancé), où toutes les options SSL/TLS sont sélectionnées. En s'appliquant à toutes les versions, le processus d'établissement de liaison est simplifié. Cependant, votre règle de blocage initiale empêchera toujours les connexions SSL 3.0 et TLS 1.0.
- Nous vous recommandons normalement d'utiliser Ne pas déchiffrer comme action par défaut pour la politique. Cependant, comme les connexions SSL 2.0 sont toujours gérées par l'action par défaut, vous pouvez utiliser Block (Bloquer) à la place. Toutefois, si vous souhaitez appliquer la règle Ne pas déchiffrer comme action par défaut à tout le trafic déchiffrable, créez une règle Do Not Decrypt (Ne pas déchiffrer) à la fin de la politique où vous acceptez toutes les valeurs par défaut pour les critères de correspondance du trafic. Cette règle correspondrait à toute connexion TLS prise en charge qui ne correspond pas à une règle antérieure dans le tableau et servirait de règle par défaut pour ces versions TLS.

Surveillance et dépannage du déchiffrement SSL

Les rubriques suivantes expliquent comment surveiller et résoudre les politiques de déchiffrement SSL.

Surveillance du déchiffrement SSL

Vous pouvez afficher les renseignements sur le déchiffrement dans les tableaux de bord et les événements pour le trafic qui correspond aux règles (ou à l'action par défaut) pour lesquelles vous avez activé la journalisation.

Tableau de bord du déchiffrement SSL

Pour évaluer les statistiques globales de déchiffrement, consultez le tableau de bord **Monitoring (Surveillance)** > **SSL Decryption (Déchiffrement SSL)**. Le tableau de bord affiche les informations suivantes :

- Pourcentage du trafic chiffré par rapport au trafic en texte brut.
- La quantité du trafic chiffré est déchiffrée par les règles SSL.

Événements

En plus du tableau de bord, la visionneuse d'événements (**Monitoring (Surveillance)** > **Events (Événements)**) comprend des informations SSL pour le trafic chiffré. Voici quelques conseils pour évaluer les événements :

- Pour les connexions qui ont été abandonnées parce qu'elles correspondaient à une règle SSL (ou à une action par défaut) qui a bloqué le trafic correspondant, le champ **Action** doit être « Block » (Blocage) et le **Reason** (Motif) doit indiquer « SSL Block » (Blocage SSL).

- Le champ **SSL Actual Action (Action réelle SSL)** (Syslog : SSLActualAction) indique l'action réelle que le système a appliquée à la connexion. Cette valeur peut différer de **SSL Expected Action (Action SSL attendue)** (Syslog : SSLExpectedAction), qui indique l'action définie dans la règle de correspondance. Par exemple, une connexion peut correspondre à une règle qui applique le déchiffrement, mais qui n'a pas pu être déchiffrée pour une raison quelconque.

Gestion des sites Web où la règle Decrypt Re-sign (Déchiffrer-Resigner) fonctionne pour un navigateur mais pas pour une application (SSL ou épinglage d'autorité de certification)

Certaines applications pour téléphones intelligents et autres périphériques utilisent une technique appelée épinglage SSL (Autorité de certification). La technique d'épinglage SSL intègre le hachage du certificat de serveur d'origine dans l'application elle-même. Par conséquent, lorsque l'application reçoit le certificat résigné du périphérique Firepower Threat Defense, la validation du hachage échoue et la connexion est abandonnée.

Le principal signe est que les utilisateurs ne peuvent pas se connecter au site Web à l'aide de l'application du site, mais qu'ils peuvent se connecter à l'aide du navigateur Web, même s'ils utilisent le navigateur sur le même périphérique sur lequel l'application échoue. Par exemple, les utilisateurs ne peuvent pas utiliser l'application Facebook iOS ou Android, mais ils peuvent pointer Safari ou Chrome vers https://www.facebook.com et établir une connexion avec succès.

Comme l'épinglage SSL est spécifiquement utilisé pour éviter les attaques de l'homme du milieu, il n'y a pas de solution de contournement. Vous devez choisir entre les options suivantes :

- Prenez en charge les utilisateurs de l'application, auquel cas vous ne pouvez pas déchiffrer le trafic vers le site. Créez une règle Do Not Decrypt (Ne pas déchiffrer) pour l'application du site (sous l'onglet Application de la règle de déchiffrement SSL) et assurez-vous que la règle précède toute règle Decrypt Re-sign (Déchiffrer-resigner) qui s'appliquerait aux connexions.
- Forcez les utilisateurs à utiliser uniquement les navigateurs. Si vous devez déchiffrer le trafic vers le site, vous devrez informer les utilisateurs qu'ils ne peuvent pas utiliser l'application du site lorsqu'ils se connectent sur votre réseau et qu'ils doivent utiliser uniquement leur navigateur.

Renseignements complémentaires

Si un site fonctionne dans un navigateur mais pas dans une application sur le même périphérique, il s'agit presque certainement d'une instance d'épinglage SSL. Toutefois, si vous souhaitez approfondir la recherche de la cause, vous pouvez utiliser des événements de connexion pour identifier l'épinglage SSL en plus du test du navigateur.

Une application peut gérer les échecs de validation du hachage de deux manières :

- Les applications du groupe 1, telles que Facebook, envoient un message d'alerte SSL dès qu'elles reçoivent le message CH, CERT ou SHD du serveur. L'alerte est généralement une alerte « Autorité de certification inconnue (48) » indiquant un épinglage SSL. Une réinitialisation TCP est envoyée après le message d'alerte. Vous devriez voir les symptômes suivants dans les détails de l'événement :
  - Les indicateurs de flux SSL incluent ALERT_SEEN.
  - Les indicateurs de flux SSL n'incluent pas APP_DATA_C2S ni APP_DATA_S2C.
  - Les messages de flux SSL sont généralement les suivants : CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE.

- Les applications du groupe 2, comme Dropbox, n'envoient aucune alerte. Au lieu de cela, ils attendent la fin de la prise de contact, puis envoient une réinitialisation TCP. Vous devriez voir les symptômes suivants :
  - Les indicateurs de flux SSL n'incluent pas ALERT_SEEN, APP_DATA_C2S ou APP_DATA_S2C.
  - Les messages de flux SSL sont généralement les suivants : CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED.



CHAPITRE 19

Stratégies d'identité

Vous pouvez utiliser des politiques d'identité pour collecter des renseignements sur l'identité des utilisateurs à partir des connexions. Vous pouvez ensuite afficher l'utilisation en fonction de l'identité de l'utilisateur dans les tableaux de bord et configurer le contrôle d'accès en fonction de l'utilisateur ou du groupe d'utilisateurs.

- Aperçu de la politique d'identité, à la page 475
- Comment mettre en œuvre la politique d'identité, à la page 477
- Configuration des politiques d'identité, à la page 478
- Activation de l'authentification transparente de l'utilisateur, à la page 485
- Politiques d'identité de surveillance, à la page 488
- Exemples de politiques d'identité, à la page 489

Aperçu de la politique d'identité

Vous pouvez utiliser les politiques d'identité pour détecter l'utilisateur associé à une connexion. En identifiant l'utilisateur, vous pouvez corréler les informations sur les menaces, les points terminaux et le réseau avec les informations d'identité de l'utilisateur. En associant le comportement, le trafic et les événements du réseau directement à chaque utilisateur, le système peut vous aider à déterminer la source des violations des politiques, des attaques ou des vulnérabilités du réseau.

Par exemple, vous pouvez identifier à qui appartient l'hôte ciblé par un incident d'intrusion et qui a lancé une attaque interne ou un balayage de port. Vous pouvez également identifier les utilisateurs à bande passante élevée et les utilisateurs qui accèdent à des sites Web ou à des applications indésirables.

La détection des utilisateurs va au-delà de la collecte de données pour l'analyse. Vous pouvez également définir des critères d'accès en fonction du nom d'utilisateur ou du nom de groupe d'utilisateurs, afin d'autoriser ou de bloquer sélectivement l'accès aux ressources selon l'identité de l'utilisateur.

Vous pouvez obtenir l'identité de l'utilisateur à l'aide des méthodes suivantes :

- Authentification passive—Pour tous les types de connexions, obtenez l'identité de l'utilisateur à partir d'autres services d'authentification sans demander le nom d'utilisateur et le mot de passe.
- Authentification active : pour les connexions HTTP uniquement, demandez le nom d'utilisateur et le mot de passe et authentifiez-vous auprès de la source d'identité indiquée afin d'obtenir l'identité de l'utilisateur pour l'adresse IP source.

Pour plus d'informations, consultez les rubriques suivantes.

Établissement de l'identité de l'utilisateur par l'authentification passive

L'authentification passive recueille l'identité de l'utilisateur sans lui demander son nom d'utilisateur et son mot de passe. Le système obtient les mappages à partir des sources d'identité que vous indiquez.

Vous pouvez obtenir de manière passive des mappages utilisateur-adresse IP à partir des sources suivantes :

- Connexions VPN d'accès à distance. Les types d'utilisateurs suivants sont pris en charge pour l'identité passive :
  - Comptes d'utilisateur définis dans un serveur d'authentification externe.
  - Les comptes d'utilisateurs locaux qui sont définis dans le Gestionnaire de périphériques de pare-feu.
- Cisco Identity Services Engine (ISE) ; Cisco Identity Services Engine Passive Identity Connector (ISE PIC).

Si un utilisateur donné est identifié par plusieurs sources, l'identité du VPN d'accès à distance prévaut.

Établissement de l'identité de l'utilisateur par l'authentification active

L'authentification est l'action de confirmer l'identité d'un utilisateur.

Avec l'authentification active, lorsqu'un flux de trafic HTTP provient d'une adresse IP pour laquelle le système ne dispose d'aucun mappage d'identité d'utilisateur, vous pouvez décider d'authentifier ou non l'utilisateur à l'origine du flux de trafic auprès du répertoire configuré pour le système. Si l'utilisateur s'authentifie avec succès, l'adresse IP est considérée comme ayant l'identité de l'utilisateur authentifié.

L'échec de l'authentification n'affecte pas l'accès au réseau pour l'utilisateur. Ce sont vos critères d'accès qui déterminent en dernier ressort le niveau d'accès accordé à ces utilisateurs.

Traiter avec des utilisateurs inconnus

Lorsque vous configurez le serveur de répertoire pour la politique d'identité, le système télécharge les informations d'appartenance des utilisateurs et des groupes à partir du serveur de répertoire. Ces informations sont actualisées toutes les 24 heures à zéro, ou chaque fois que vous modifiez et enregistrez la configuration du répertoire (même si vous n'apportez aucune modification).

Si un utilisateur réussit à s'authentifier lorsqu'il est invité par une règle d'identité d'authentification active, mais que le nom de l'utilisateur ne figure pas dans les informations d'identité de l'utilisateur téléchargées, l'utilisateur est marqué comme Inconnu. Vous ne verrez pas l'ID de l'utilisateur dans les tableaux de bord liés à l'identité, et l'utilisateur ne correspondra pas aux règles de groupe.

Cependant, toutes les règles de contrôle d'accès pour l'utilisateur inconnu s'appliqueront. Par exemple, si vous bloquez les connexions pour les utilisateurs inconnus, ces utilisateurs sont bloqués même s'ils ont réussi à s'authentifier (ce qui signifie que le serveur de répertoire reconnaît l'utilisateur et que le mot de passe est valide).

Ainsi, lorsque vous apportez des modifications au serveur de répertoire, comme l'ajout ou la suppression d'utilisateurs, ou la modification de l'appartenance à un groupe, ces modifications ne sont pas répercutées dans l'application des politiques tant que le système n'a pas téléchargé les mises à jour à partir du répertoire.

Si vous ne souhaitez pas attendre la mise à jour quotidienne de minuit, vous pouvez forcer une mise à jour en modifiant les informations de domaine du répertoire (à partir de **Objects (Objets)** > **Identity Sources (Sources**

d'identité), puis modifiez le domaine). Cliquez sur **Save** (Enregistrer), puis déployez les modifications. Le système téléchargera immédiatement les mises à jour.



Remarque Vous pouvez vérifier si des informations d'utilisateur nouvelles ou supprimées se trouvent sur le système en vous rendant dans **Policies (Politiques)** > **Access Control (Contrôle d'accès)**, en cliquant sur le bouton **Add Rule (Ajouter une règle) (+)**, puis en consultant la liste des utilisateurs sous l'onglet **Users (Utilisateurs)**. Si vous ne trouvez pas un nouvel utilisateur ou si vous trouvez un utilisateur supprimé, le système dispose d'informations obsolètes.

Comment mettre en œuvre la politique d'identité

Pour activer l'acquisition de l'identité de l'utilisateur, afin que l'utilisateur associé à une adresse IP soit connu, vous devez configurer plusieurs éléments. Lorsqu'il est configuré correctement, vous pourrez voir les noms d'utilisateur dans les tableaux de bord et les événements de surveillance. Vous pourrez également utiliser l'identité de l'utilisateur dans les règles de contrôle d'accès et de déchiffrement SSL comme critère de correspondance du trafic.

La procédure suivante fournit un aperçu de ce que vous devez configurer pour que les politiques d'identité fonctionnent.

Procédure

Étape 1 Configurez le domaine d'identité AD.

Que vous collectiez l'identité de l'utilisateur de manière active (en invitant à l'authentification de l'utilisateur) ou passive, vous devez configurer le serveur Active Directory (AD) qui dispose des informations d'identité de l'utilisateur. Consultez Configuration des domaines d'identité AD, à la page 171.

Si vous configurez l'identité passive, vous pouvez créer des séquences de domaine AD qui permettent au système d'extraire les identités de plusieurs domaines AD. Cette fonction est utile si vous avez plusieurs domaines AD dans votre réseau.

Étape 2 Si vous souhaitez utiliser des règles d'identité d'authentification passive, configurez les sources d'identité passive.

Vous pouvez configurer l'un des éléments suivants, en fonction des services que vous mettez en œuvre dans le périphérique et des services disponibles dans votre réseau.

- VPN d'accès à distance : si vous avez l'intention de prendre en charge les connexions VPN d'accès à distance sur le périphérique, les connexions d'utilisateur peuvent fournir l'identité en fonction du serveur AD ou des utilisateurs locaux (ceux définis dans Gestionnaire de périphériques de pare-feu). Pour en savoir plus sur la configuration du VPN d'accès à distance, consultez Configuration du VPN d'accès à distance, à la page 711.
- Cisco Identity Services Engine (ISE) ou Cisco Identity Services Engine Passive Identity Connector (ISE PIC) : si vous utilisez ces produits, vous pouvez configurer l'appareil en tant qu'abonné pxGrid et obtenir l'identité de l'utilisateur auprès d'ISE. Consultez Configurer Identity Services Engine (ISE), à la page 181.

Étape 3 Choisissez **Policies (Politiques)** > **Identity (Identité)**, et activez la politique d'identité. Consultez Configuration des politiques d'identité, à la page 478.

Étape 4 Configurer les paramètres de la politique d'identité, à la page 479.

Les sources d'identité passives sont automatiquement sélectionnées en fonction des sources que vous avez configurées dans le système. Si vous souhaitez configurer l'authentification active, vous devez configurer les certificats pour le portail captif et le déchiffrement avec nouvelle signature SSL (si vous n'avez pas encore activé la politique de déchiffrement SSL).

Étape 5 Configurer l'action par défaut de la politique d'identité, à la page 480.

Si votre intention est d'utiliser uniquement l'authentification passive, vous pouvez définir l'action par défaut sur l'authentification passive et il n'est pas nécessaire de créer des règles spécifiques.

Étape 6 Configurer les règles d'identité, à la page 481.

Créez des règles qui collecteront les identités d'utilisateurs passives ou actives à partir des réseaux concernés.

Configuration des politiques d'identité

Vous pouvez utiliser des politiques d'identité pour collecter des renseignements sur l'identité des utilisateurs à partir des connexions. Vous pouvez ensuite afficher l'utilisation en fonction de l'identité de l'utilisateur dans les tableaux de bord et configurer le contrôle d'accès en fonction de l'utilisateur ou du groupe d'utilisateurs.

Voici un aperçu de la configuration des éléments requis pour obtenir l'identité de l'utilisateur au moyen des politiques d'identité.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Identity (identité)**.

Si vous n'avez pas encore défini de politique d'identité, cliquez sur **Enable Identity Policy** (Activer la politique d'identité) et configurez les paramètres comme décrit dans Configurer les paramètres de la politique d'identité, à la page 479.

Étape 2 Gérer la politique d'identité.

Une fois que vous avez configuré les paramètres d'identité, cette page répertorie toutes les règles dans l'ordre. Les règles sont comparées au trafic du haut vers le bas, la première correspondance détermine l'action à appliquer. Vous pouvez effectuer ce qui suit à partir de cette page :

- Pour activer ou désactiver la politique d'identité, cliquez sur le bouton à bascule **Identity Policy** (Politique d'identité).
- Pour modifier les paramètres de la politique d'identité, cliquez sur le bouton **Identity Policy Configuration** (Configuration de la politique d'identité) ( ).
- Pour modifier **Default Action** (Action par défaut), cliquez sur l'action et sélectionnez l'action souhaitée. Consultez Configurer l'action par défaut de la politique d'identité, à la page 480.

- Pour déplacer une règle, modifiez-la et sélectionnez le nouvel emplacement dans la liste déroulante **Order** (Ordre).
- Pour configurer des règles :
  - Pour créer une nouvelle règle, cliquez sur le bouton +.
  - Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle (dans la colonne Actions). Vous pouvez également modifier de manière sélective une propriété de règle en cliquant sur la propriété dans le tableau.
  - Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression ( ) de la règle (dans la colonne Actions).

Pour plus d'informations sur la création et la modification des règles d'identité, consultez Configurer les règles d'identité, à la page 481.

Configurer les paramètres de la politique d'identité

Pour que les politiques d'identité fonctionnent, vous devez configurer les sources qui fournissent des informations sur l'identité de l'utilisateur. Les paramètres que vous devez configurer varient selon le type de règles que vous configurez : passives, actives ou les deux.

La boîte de dialogue des paramètres affiche ces paramètres dans des sections distinctes. Selon la façon dont vous accédez à la boîte de dialogue, vous verrez les deux sections ou une seule section. La boîte de dialogue s'affiche automatiquement si vous essayez de créer une règle pour un type d'authentification sans avoir déjà configuré les paramètres requis.

La procédure suivante couvre la boîte de dialogue complète.

Avant de commencer

Vérifiez que les paramètres d'horloge sont uniformes pour les serveurs d'annuaire, le périphérique Firewall Threat Defense et les clients. Un décalage temporel entre ces périphériques peut empêcher l'authentification de l'utilisateur réussie. « cohérence » signifie que vous pouvez utiliser différents fuseaux horaires, mais que l'heure doit être la même pour ces fuseaux horaires; par exemple, 10 h HNP = 13 h HNE.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Identity (identité)**.

Étape 2 Cliquez sur le bouton **Identity Policy Configuration** ( ).

Étape 3 Configurez les options **d'authentification passive**.

La boîte de dialogue vous affiche les sources d'authentification passive que vous avez déjà configurées.

Si nécessaire, vous pouvez configurer ISE à partir de cette boîte de dialogue. Si vous n'avez pas encore configuré d'objet ISE, vous pouvez cliquer sur le lien **Integrate ISE** (intégrer ISE) et le créer maintenant. Si l'objet existe, il est répertorié avec son état : Enabled (activé) ou Disabled (désactivé).

Vous devez avoir configuré au moins une source d'identité passive pour créer des règles d'authentification passive.

Étape 4 Configurez les options **d'authentification active**.

Lorsqu'une règle d'identité requiert une authentification active pour un utilisateur, l'utilisateur est redirigé vers le port du portail captif de l'interface par laquelle il est connecté, puis il est invité à s'authentifier.

- **Server Certificate** (certificat de serveur) : Sélectionnez le certificat interne à présenter aux utilisateurs lors de l'authentification active. Si vous n'avez pas encore créé le certificat requis, cliquez sur **Create New Internal Certificate** (créer un nouveau certificat interne) dans la partie inférieure de la liste déroulante.

  Les utilisateurs devront accepter le certificat si vous ne téléchargez pas un certificat déjà réputé fiable pour leurs navigateurs.

- **Port** : le port du portail captif. La valeur par défaut est 885 (TCP). Si vous configurez un autre port, il doit être compris entre 1025 et 65535.

  Remarque
  Pour les méthodes d'authentification HTTP de base, la page de réponse HTTP et NTLM, l'utilisateur est redirigé vers le portail captif en utilisant l'adresse IP de l'interface. Toutefois, pour la négociation HTTP, l'utilisateur est redirigé à l'aide du nom DNS complet *firewall-hostname.AD-domain-name*. Si vous souhaitez utiliser la négociation HTTP, vous devez également mettre à jour votre serveur DNS pour mapper ce nom aux adresses IP de toutes les interfaces internes pour lesquelles une authentification active est requise. Sinon, la redirection ne peut pas être terminée et les utilisateurs ne peuvent pas s'authentifier.

Étape 5 (Authentification active seulement) Dans **Decrypt Re-Sign Certificate** (Déchiffrer le certificat re-signé), sélectionnez le certificat d'autorité de certification interne à utiliser pour les règles mettant en œuvre le déchiffrement avec des certificats re-signés.

Vous pouvez utiliser le certificat NGFW-Default-InternalCA prédéfini ou celui que vous avez créé ou téléversé. Si le certificat n'existe pas encore, cliquez sur **Create Internal CA** (créer une autorité de certification interne) pour le créer.

Si vous n'avez pas encore installé le certificat dans les navigateurs clients, cliquez sur le bouton de téléchargement () pour en obtenir une copie. Consultez la documentation de chaque navigateur afin de savoir comment installer le certificat. Voir aussi Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature, à la page 469.

Remarque
Vous êtes invité à saisir les paramètres de déchiffrement SSL uniquement si vous n'avez pas encore configuré la politique de déchiffrement SSL. Pour modifier ces paramètres après avoir activé la politique d'identité, modifiez les paramètres de politique de déchiffrement SSL.

Étape 6 Cliquez sur **Save** (Enregistrer).

Configurer l'action par défaut de la politique d'identité

La politique d'identité a une action par défaut, qui est mise en œuvre pour les connexions qui ne correspondent à aucune règle d'identité individuelle.

En fait, l'absence de règle est une configuration valide pour votre politique. Si vous avez l'intention d'utiliser l'authentification passive sur toutes les sources de trafic, configurez simplement l'authentification passive comme action par défaut.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Identity (identité)**.

Étape 2 Cliquez dans **Default Action** (Action par défaut) et choisissez l'une des options suivantes :

- **Passive Auth** (Any Identity Source) (toute source d'identité) : l'identité de l'utilisateur est déterminée à l'aide de toutes les sources d'identité passive configurées pour les connexions qui ne correspondent à aucune règle d'identité. Si vous ne configurez aucune source d'identité passive, l'utilisation de Passive Auth comme action par défaut équivaut à l'utilisation de No Auth.
- **No Auth** (No Authentication Required) : l'identité de l'utilisateur n'est pas déterminée pour les connexions qui ne correspondent à aucune règle d'identité.

Configurer les règles d'identité

Les règles d'identité déterminent si les informations d'identité d'utilisateur doivent être recueillies pour le trafic correspondant. Vous pouvez configurer No Authentication (aucune authentification) si vous ne souhaitez pas obtenir les informations d'identité de l'utilisateur pour le trafic correspondant.

N'oubliez pas que quelle que soit la configuration de votre règle, l'authentification active est effectuée uniquement sur le trafic HTTP. Ainsi, vous n'avez pas besoin de créer des règles pour exclure de l'authentification active le trafic ne relevant pas de HTTP. Vous pouvez simplement appliquer une règle d'authentification active à toutes les sources et destinations si vous souhaitez obtenir des informations d'identité utilisateur pour tout le trafic HTTP.



Remarque Gardez également à l'esprit qu'un échec de l'authentification n'a aucune incidence sur l'accès au réseau. Les politiques d'identité recueillent uniquement les informations d'identité de l'utilisateur. Vous devez utiliser des règles d'accès si vous souhaitez empêcher les utilisateurs qui n'ont pas pu s'authentifier d'accéder au réseau.

Avant de commencer

Les règles sont évaluées de haut en bas. Pour une connexion qui correspond aux critères de réseau spécifiés d'une règle donnée, l'utilisateur est évalué par rapport au domaine d'identité spécifié dans la règle. Si l'utilisateur ne fait pas partie de ce domaine, il sera marqué comme inconnu et aucune autre règle de la politique d'identité ne sera évaluée. Par conséquent, si vous avez plusieurs domaines qui doivent être évalués, assurez-vous d'utiliser des séquences de domaines au lieu d'un seul domaine.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Identity (identité)**.

Étape 2 Effectuez l'une des actions suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle.

Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression ( ) de la règle.

Étape 3 Sous **Order**, sélectionnez l'endroit où vous souhaitez insérer la règle dans la liste ordonnée des règles.

Les règles sont appliquées sur la base de la première correspondance, vous devez donc vous assurer que les règles comprenant des critères de correspondance de trafic très spécifiques apparaissent au-dessus des politiques qui ont des critères plus généraux, qui s'appliqueraient autrement au trafic correspondant.

La valeur par défaut consiste à ajouter la règle à la fin de la liste. Si vous souhaitez modifier l'emplacement d'une règle ultérieurement, modifiez cette option.

Étape 4 Dans **Title** (titre), entrez un nom pour la règle.

Étape 5 Sélectionnez **Action** et, si nécessaire, la source d'identité AD (**AD Identity Source**).

Vous devez sélectionner le domaine d'identité AD qui comprend les comptes d'utilisateur pour les règles d'authentification passive et active. Si le domaine n'existe pas encore, cliquez sur **Create New Identity Realm** (créer un nouveau domaine d'identité) pour le créer maintenant. Pour l'authentification passive, vous pouvez sélectionner une séquence de domaine AD plutôt qu'un seul objet de domaine AD.

- **Passive Auth** : Utilisez l'authentification passive pour déterminer l'identité de l'utilisateur. Toutes les sources d'identité configurées sont affichées. La règle utilise automatiquement toutes les sources configurées.
- **Active Auth** : Utilisez l'authentification active pour déterminer l'identité de l'utilisateur. L'authentification active est appliquée uniquement au trafic HTTP de . Si un autre type de trafic correspond à une politique d'identité nécessitant ou autorisant une authentification active, l'authentification active ne sera pas tentée.
- **No Auth** : N'obtient pas d'information sur l'identité de l'utilisateur. Les règles d'accès basées sur l'identité ne seront pas appliquées à ce trafic. Ces utilisateurs sont marqués comme **No Authentication Required** (aucune authentification requise).

Étape 6 (Authentification active seulement) Sélectionnez la méthode d'authentification (**Type**) prise en charge par votre serveur d'annuaire.

- **HTTP de base** : Authentifiez les utilisateurs qui utilisent une connexion d'authentification de base HTTP non chiffrée. Les utilisateurs se connectent au réseau en utilisant la fenêtre contextuelle d'authentification par défaut de leur navigateur. Il s'agit du paramètre par défaut.
- **NTLM** : Authentifiez les utilisateurs qui utilisent une connexion NT LAN Manager (NTLM). Cette sélection est uniquement disponible lorsque vous sélectionnez un domaine AD. Les utilisateurs se connectent au réseau à l'aide de la fenêtre contextuelle d'authentification par défaut de leur navigateur. Vous pouvez aussi configurer les navigateurs IE et Firefox pour l'authentification transparente à l'aide du nom de domaine Windows (voir Activation de l'authentification transparente de l'utilisateur, à la page 485).
- **Négociation HTTP** : Permet au périphérique de négocier la méthode entre l'agent utilisateur (l'application utilisée par l'utilisateur pour lancer le flux de trafic) et le serveur Active Directory. La négociation donne

lieu à l'utilisation de la méthode la plus efficace communément prise en charge, dans l'ordre suivant : NTLM, puis la méthode de base. Les utilisateurs se connectent au réseau en utilisant la fenêtre contextuelle d'authentification par défaut de leur navigateur.

- **Page de réponse HTTP** : Invite les utilisateurs à s'authentifier à l'aide d'une page Web fournie par le système. Il s'agit d'une forme d'authentification HTTP de base.

Remarque
Pour les méthodes d'authentification HTTP de base, la page de réponse HTTP et NTLM, l'utilisateur est redirigé vers le portail captif en utilisant l'adresse IP de l'interface. Toutefois, pour la négociation HTTP, l'utilisateur est redirigé à l'aide du nom DNS complet *firewall-hostname.AD-domain-name*. Si vous souhaitez utiliser la négociation HTTP, vous devez également mettre à jour votre serveur DNS pour mapper ce nom aux adresses IP de toutes les interfaces internes pour lesquelles une authentification active est requise. Sinon, la redirection ne peut pas être terminée et les utilisateurs ne peuvent pas s'authentifier.

Étape 7 (Authentification active seulement) Sélectionnez **Fall Back as Guest** > **On/Off** (activer/désactiver le mode Invité) pour déterminer si les utilisateurs qui échouent à l'authentification active sont étiquetés comme des utilisateurs invités.

Les utilisateurs ont trois chances de s'authentifier. Si elles échouent, votre sélection pour cette option détermine la façon dont l'utilisateur est marqué. Vous pouvez écrire des règles d'accès en fonction de ces valeurs.

- **Fall Back as Guest (basculement au mode d'invité)** > **On (activé)** Les utilisateurs sont marqués en tant qu'invité (**Guest**).
- **Fall Back as Guest (basculement au mode d'invité)** > **Off (désactivé)** Les utilisateurs sont marqués en tant qu'authentification échouée (**Failed Authentication**).

Étape 8 Définissez les critères de correspondance du trafic sous l'onglet **Source/Destination**.

N'oubliez pas que l'authentification active sera tentée uniquement avec le trafic HTTP. Par conséquent, il n'est pas nécessaire de configurer des règles entraînant la non-authentification pour le trafic en dehors du HTTP, et il est inutile de créer des règles d'authentification active pour tout trafic en dehors du HTTP. Cependant, l'authentification passive est valide pour tout type de trafic.

Les critères Source/Destination d'une règle d'identité définissent les zones de sécurité (interfaces) par lesquelles passe le trafic, les adresses IP ou le pays ou le continent (emplacement géographique) pour l'adresse IP, ou les protocoles et les ports utilisés dans le trafic. La valeur par défaut englobe toute zone ou adresse et tout emplacement géographique, protocole et port.

Pour modifier une condition, vous cliquez sur le bouton **+** dans cette condition, sélectionnez l'objet ou l'élément souhaité, puis cliquez sur **OK** dans la boîte de dialogue contextuelle. Si le critère requiert un objet, vous pouvez cliquer sur **Create New *Object*** (créer un nouvel objet) si l'objet requis n'existe pas. Cliquez sur le **x** d'un objet ou d'un élément pour le supprimer de la politique.

Vous pouvez configurer les critères de correspondance de trafic suivants.

Zones source, zones de destination

Les objets de la zone de sécurité qui définissent les interfaces par lesquelles passe le trafic. Vous pouvez définir un critère, les deux critères ou aucun critère : tout critère non spécifié s'applique au trafic sur n'importe quelle interface.

- Pour faire correspondre le trafic sortant de l'appareil depuis une interface dans la zone, ajoutez cette zone aux **zones de destination**.

- Pour faire correspondre le trafic entrant dans l'appareil depuis une interface dans la zone, ajoutez cette zone aux zones source (**Source Zones**).
- Si vous ajoutez des conditions de zone source et de zone de destination à une règle, le trafic correspondant doit provenir de l'une des zones source spécifiées et sortir par l'une des zones de destination.

Utilisez ces critères lorsque la règle doit être appliquée en fonction de l'entrée ou de la sortie du trafic sur l'appareil. Par exemple, si vous voulez vous assurer que l'information sur l'identité de l'utilisateur soit collectée à partir de tout le trafic provenant des réseaux internes, sélectionnez une zone interne comme zones source (**Source Zones**) tout en laissant la zone de destination vide.

Remarque
Vous ne pouvez pas combiner des zones de sécurité passives et routées dans une seule règle. En outre, vous pouvez spécifier des zones de sécurité passives comme zones source uniquement, vous ne pouvez pas les spécifier comme zones de destination.

Réseaux sources, réseaux de destination

Les objets réseau ou les emplacements géographiques qui définissent les adresses réseau ou les emplacements du trafic.

- Pour faire correspondre le trafic d'une adresse IP ou d'un emplacement géographique, configurez les réseaux sources (**Source Networks**).
- Pour faire correspondre le trafic à une adresse IP ou à un emplacement géographique, configurez les réseaux de destination (**Source Networks**).
- Si vous ajoutez des conditions de réseau source et de destination à une règle, le trafic correspondant doit provenir de l'une des adresses IP spécifiées et être destiné à l'une des adresses IP de destination.

Lorsque vous ajoutez ce critère, vous sélectionnez les onglets suivants :

- **Network** (réseau) : Sélectionnez les objets ou groupes réseau qui définissent les adresses IP source ou de destination du trafic que vous souhaitez contrôler.
- **Geolocation** (géolocalisation) : Sélectionnez l'emplacement géographique pour contrôler le trafic en fonction de son pays ou continent de source ou de destination. La sélection d'un continent sélectionne tous les pays du continent. En plus de sélectionner l'emplacement géographique directement dans la règle, vous pouvez également sélectionner un objet de géolocalisation que vous avez créé pour définir l'emplacement. En utilisant la localisation géographique, vous pouvez facilement restreindre l'accès à un pays en particulier sans avoir besoin de connaître toutes les adresses IP potentielles qui y sont utilisées.

  Remarque
  Pour vous assurer que vous utilisez des données de localisation géographique à jour pour filtrer votre trafic, Cisco vous recommande fortement de mettre à jour régulièrement la base de données de géolocalisation (GeoDB).

Ports source, ports/protocoles de destination

Les objets de port qui définissent les protocoles utilisés dans le trafic. Pour TCP/UDP, cela peut inclure les ports.

- Pour faire correspondre le trafic d'un protocole ou d'un port, configurez les ports source (**Source Ports**). Les ports source peuvent uniquement être TCP/UDP.

- Pour faire correspondre le trafic à un protocole ou à un port, configurez les protocoles/ports de destination (**Destination Ports/Protocols**).
- Pour faire correspondre le trafic provenant de ports TCP/UDP spécifiques et destiné à des ports TCP/UDP spécifiques, configurez les deux. Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP. Par exemple, vous pouvez cibler le trafic du port TCP/80 au port TCP/8080.

Étape 9 Cliquez sur **OK**.

Activation de l'authentification transparente de l'utilisateur

Si vous configurez la politique d'identité pour permettre l'authentification active, vous pouvez utiliser les méthodes d'authentification suivantes pour obtenir l'identité de l'utilisateur :

HTTP de base

Avec l'authentification de base HTTP, les utilisateurs sont toujours invités à s'authentifier avec leur nom d'utilisateur et leur mot de passe de répertoire. Le mot de passe est transmis en texte clair. Pour cette raison, l'authentification de base n'est pas considérée comme une forme d'authentification sécurisée.

L'authentification de base est le mécanisme d'authentification par défaut.

Page de réponse HTTP

C'est un type d'authentification HTTP de base, suivant lequel l'utilisateur se voit présenter une page de navigateur de connexion.

NTLM, HTTP Negotiate (authentification Windows intégrée pour Active Directory)

Grâce à l'authentification Windows intégrée, vous profitez du fait que les utilisateurs se connectent à un domaine pour utiliser leur poste de travail. Le navigateur tente d'utiliser cette connexion de domaine lors de l'accès à un serveur, y compris au portail captif de Firepower Threat Defense lors de l'authentification active. Le mot de passe n'est pas transmis. Si l'authentification réussit, l'utilisateur est authentifié de manière transparente; l'utilisateur n'est au courant d'aucun défi d'authentification.

Si le navigateur ne peut pas répondre à une demande d'authentification à l'aide des identifiants de connexion au domaine, l'utilisateur est invité à entrer son nom d'utilisateur et son mot de passe, ce qui correspond à l'expérience utilisateur de l'authentification de base. Ainsi, si vous configurez l'authentification Windows intégrée, cela peut réduire le besoin pour les utilisateurs de fournir des identifiants lors de l'accès au réseau ou aux serveurs dans le même domaine.

Il convient de signaler que HTTP Negotiate choisit la méthode la plus efficace prise en charge par le serveur Active Directory et l'agent utilisateur. Si la négociation sélectionne HTTP de base comme méthode d'authentification, vous n'obtiendrez pas une authentification transparente. L'ordre de priorité va comme suit : NTLM, puis authentification de base. La négociation doit sélectionner NTLM pour que l'authentification transparente soit possible.

Vous devez configurer les navigateurs clients pour prendre en charge l'authentification Windows intégrée afin de permettre une authentification transparente. Les sections suivantes expliquent les exigences générales et la configuration de base de l'authentification Windows intégrée pour certains navigateurs couramment utilisés qui la prennent en charge. Les utilisateurs doivent consulter les rubriques d'aide de leur navigateur (ou d'un autre agent utilisateur) pour obtenir des renseignements plus détaillés, car les techniques peuvent changer selon les versions de logiciels.

Astuces Tous les navigateurs ne prennent pas en charge l'authentification Windows intégrée, par exemple, Chrome et Safari (selon les versions disponibles au moment de la rédaction). Un nom d'utilisateur et un mot de passe seront demandés aux utilisateurs. Consultez la documentation du navigateur pour déterminer si une assistance est disponible dans la version que vous utilisez.

Exigences pour l'authentification transparente

Les utilisateurs doivent configurer leur navigateur ou leur agent utilisateur pour mettre en œuvre l'authentification transparente. Ils peuvent le faire individuellement ou vous pouvez le configurer pour eux et envoyer la configuration aux postes de travail clients à l'aide de vos outils de distribution de logiciels. Si vous décidez de laisser les utilisateurs le faire eux-mêmes, veillez à fournir les paramètres de configuration spécifiques qui fonctionnent pour votre réseau.

Quels que soient le navigateur ou l'agent utilisateur, vous devez mettre en œuvre la configuration générale suivante :

- Ajoutez l'interface Firepower Threat Defense par laquelle les utilisateurs se connectent au réseau à la liste des Trusted Sites (sites de confiance). Vous pouvez utiliser l'adresse IP ou, si disponible, le nom de domaine complet (par exemple : interne.exemple.com). Vous pouvez également utiliser des caractères génériques ou des adresses partielles pour créer un site de confiance généralisé. Par exemple, vous pouvez généralement couvrir tous les sites internes en utilisant *.example.com ou simplement exemple.com, en faisant confiance à tous les serveurs de votre réseau (utilisez votre propre nom de domaine). Si vous ajoutez l'adresse spécifique de l'interface, vous devrez peut-être ajouter plusieurs adresses aux sites de confiance pour prendre en compte tous les points d'accès des utilisateurs au réseau.
- L'authentification Windows intégrée ne fonctionne pas par l'intermédiaire d'un serveur mandataire. Par conséquent, vous devez soit ne pas utiliser de serveur mandataire, soit ajouter le Firepower Threat Defenseaux adresses exclues du passage par le serveur mandataire. Si vous décidez que vous devez utiliser un serveur mandataire, les utilisateurs seront invités à s'authentifier même si vous utilisez NTLM.

Astuces La configuration de l'authentification transparente n'est pas une exigence, mais une commodité pour les utilisateurs finaux. Si vous ne configurez pas l'authentification transparente, les utilisateurs reçoivent un défi de connexion pour toutes les méthodes d'authentification.

Configuration d'Internet Explorer pour l'authentification transparente

Pour configurer Internet Explorer pour l'authentification transparente NTLM :

Procédure

Étape 1 Sélectionnez **Tools (Outils) > Internet Options (Options Internet)**.

Étape 2 Sélectionnez l'onglet **Security** (Sécurité), sélectionnez la zone **Local Intranet** (Intranet local), puis procédez comme suit :

a) Cliquez sur le bouton **Sites** pour ouvrir la liste des sites de confiance.

b) Assurez-vous qu'au moins une des options suivantes est sélectionnée :

- **Automatically detect intranet network** (Détecter automatiquement le réseau intranet). Si vous sélectionnez cette option, toutes les autres options sont désactivées.
- **Include all sites that bypass the proxy** (Inclure tous les sites qui contournent le serveur mandataire).

c) Cliquez sur **Advanced (Avancé)** pour ouvrir la boîte de dialogue Sites intranet locaux, puis collez l'URL à approuver dans la zone **Add Site (Ajouter un site)** et cliquez sur **Add (Ajouter)**.

Répétez le processus si vous avez plusieurs URL. Utilisez des caractères génériques pour spécifier une URL partielle, comme **`http://*.exemple.com`** ou simplement **`*.exemple.com`**.

Fermez les boîtes de dialogue pour revenir à la boîte de dialogue des options Internet.

d) Avec **Local Intranet** (Intranet local) toujours sélectionné, cliquez sur **Custom Level** (Niveau personnalisé) pour ouvrir la boîte de dialogue Security Settings (Paramètres de sécurité). Recherchez le paramètre **User Authentication (Authentification utilisateur)** > **Logon (Connexion)** et sélectionnez **Automatic logon only in Intranet zone** (Connexion automatique uniquement dans la zone Intranet). Cliquez sur **OK**.

Étape 3 Dans la boîte de dialogue Internet Options, cliquez sur l'onglet **Connections** (Connexions), puis sur **LAN Settings** (Paramètres réseau local).

Si **Use a proxy server for your LAN** (Utiliser un serveur mandataire pour votre réseau local) est sélectionné, vous devez vous assurer que l'interface Firepower Threat Defense contourne le proxy. Effectuez l'une des actions suivantes, le cas échéant :

- Sélectionnez **Bypass proxy server for local addresses (Contourner le serveur proxy pour les adresses locales)**.
- Cliquez sur **Advanced** (Avancé) et saisissez l'adresse dans la zone **Do not use proxy server for addresses beginning with** (Ne pas utiliser de serveur proxy pour les adresses commençant par). Vous pouvez utiliser des caractères génériques, par exemple, **`*.exemple.com`**.

Configuration de Firefox pour l'authentification transparente

Configurer Firefox pour l'authentification transparente NTLM :

Procédure

Étape 1 Ouvrez **about:config**. Utilisez la barre de filtres pour vous aider à localiser les préférences que vous devez modifier.

Étape 2 Pour prendre en charge NTLM, modifiez les préférences suivantes (filtre sur network.automatic) :

- **network.automatic-ntlm-auth.trusted-uris** : double-cliquez sur la préférence, saisissez l'URL et cliquez sur **OK**. Vous pouvez saisir plusieurs URL en les séparant par des virgules ; le protocole peut être omis. Par exemple :

```
http://host.example.com, http://hostname, myhost.example.com
```

Vous pouvez également utiliser des URL partielles. Firefox correspond à la fin de la chaîne, et non à une sous-chaîne aléatoire. Ainsi, vous pouvez inclure l'ensemble de votre réseau interne en précisant uniquement votre nom de domaine. Par exemple :

```
example.com
```

- **network.automatic-ntlm-auth.allow-proxies** : vérifiez que la valeur est **true**, qui est la valeur par défaut. Double-cliquez pour modifier la valeur si elle est actuellement false.

Étape 3 Vérifiez les paramètres du serveur mandataire HTTP. Vous pouvez les trouver en sélectionnant **Tools (Outils)** > **Options**, puis en cliquant sur l'onglet **Network** (Réseau) dans la boîte de dialogue des options. Cliquez sur le bouton **Settings** (paramètres) dans le groupe Connection (connexion).

- Si **No Proxy** (Aucun mandataire) est sélectionné, il n'y a rien à configurer.
- Si **Use System Proxy Settings** (Utiliser les paramètres de mandataire du système) est sélectionné, vous devez modifier la propriété **network.proxy.no_proxies_on** dans about:config pour ajouter les URI de confiance que vous avez inclus dans **network.automatic-ntlm-auth.trusted-uris**.
- Si **Manual Proxy Configuration** (Configuration manuelle du serveur mandataire) est sélectionnée, mettez à jour la liste **No Proxy For** (Aucun mandataire pour) pour inclure ces URI de confiance.
- Si l'une des autres options est sélectionnée, assurez-vous que les propriétés utilisées pour ces configurations excluent les mêmes URI de confiance.

Politiques d'identité de surveillance

Si les politiques d'identité qui nécessitent l'authentification fonctionnent correctement, vous devriez voir les informations sur les utilisateurs dans le tableau de bord **Monitoring (Surveillance)** > **Users (Utilisateurs)** ainsi que dans d'autres tableaux de bord qui incluent des informations utilisateur.

En outre, les événements affichés dans **Monitoring (Surveillance)** > **Events (Événements)** devraient inclure des informations utilisateur.

Si vous ne voyez aucune information d'utilisateur, vérifiez que le serveur de répertoire fonctionne correctement. Utilisez le bouton **Test** (Tester) dans la boîte de dialogue de configuration du serveur de répertoire pour vérifier la connectivité.

Si le serveur de répertoire fonctionne et est utilisable, vérifiez que les critères de correspondance du trafic dans les règles d'identité qui nécessitent une authentification active sont rédigés de manière à correspondre à vos utilisateurs. Par exemple, assurez-vous que la zone source contient les interfaces par lesquelles le trafic utilisateur entrera dans le périphérique. Les règles d'identité d'authentification active ne correspondent qu'au trafic HTTP; les utilisateurs doivent donc envoyer ce type de trafic par l'intermédiaire du périphérique.

Pour l'authentification passive, utilisez le bouton **Test** (Tester) dans l'objet ISE si vous utilisez cette source. Si vous utilisez le VPN d'accès à distance, vérifiez que le service fonctionne correctement et que les utilisateurs peuvent établir des connexions VPN. Consultez les rubriques de dépannage de ces fonctionnalités pour obtenir des renseignements plus détaillés sur l'identification et la résolution des problèmes.

Exemples de politiques d'identité

Le chapitre sur les cas d'utilisation comprend un exemple de mise en œuvre des politiques d'identité. Veuillez consulter Comment mieux comprendre le trafic de votre réseau, à la page 49.



CHAPITRE 20

Renseignements de sécurité

La politique de renseignements de sécurité vous donne l'occasion d'abandonner rapidement le trafic indésirable en fonction de l'adresse IP source/de destination ou de l'URL de destination. Les rubriques suivantes expliquent comment mettre en œuvre Security Intelligence.

- À propos des renseignements sur la sécurité, à la page 491
- Exigences de licence pour les renseignements sur la sécurité, à la page 494
- Configurer les renseignements sur la sécurité, à la page 494
- Surveillance de l'intelligence de sécurité, à la page 495
- Exemples pour les renseignements sur la sécurité, à la page 495

À propos des renseignements sur la sécurité

La politique de renseignements de sécurité vous donne l'occasion d'abandonner rapidement le trafic indésirable en fonction de l'adresse IP source/de destination ou de l'URL de destination. Le système supprime ce trafic indésirable avant de l'évaluer avec la stratégie de contrôle d'accès, réduisant ainsi la quantité de ressources système utilisées.

Vous pouvez bloquer le trafic en fonction des éléments suivants :

- Flux Cisco Talos Intelligence Group (Talos) : Talos fournit un accès à des flux de renseignements de sécurité régulièrement mis à jour. Les sites qui représentent des menaces de sécurité, comme les programmes malveillants, les pourriels, les réseaux de zombies et l'hameçonnage peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer des configurations personnalisées. Le système télécharge régulièrement des mises à jour de flux; ainsi, les nouvelles informations sur les menaces sont disponibles sans que vous ayez à redéployer la configuration.

Remarque Les flux Talos sont mis à jour par défaut toutes les heures. Vous pouvez modifier la fréquence de mise à jour et même mettre à jour les flux à la demande à partir de la page **Device (Périphérique)** > **Updates (Mises à jour)**.

- Network and URL Objects (Objets de réseau et d'URL) : si vous connaissez des adresses IP ou des URL spécifiques que vous souhaitez bloquer, vous pouvez créer des objets pour celles-ci et les ajouter à la liste des adresses bloquées ou à la liste des autorisations. Notez que vous ne pouvez pas utiliser d'objets réseau avec des spécifications de FQDN (nom de domaine complet) ou de plage.

Vous créez des listes distinctes pour les adresses IP (réseaux) et les URL.

Remarque Si une demande HTTP/HTTPS s'adresse à une URL qui utilise une adresse IP au lieu d'un nom d'hôte, le système recherche la réputation de l'adresse IP dans les listes d'adresses réseau. Vous n'avez pas besoin de dupliquer les adresses IP dans les listes de réseaux et d'URL.

Création d'exceptions aux listes de blocage

Pour chaque liste de blocage, vous pouvez créer une liste d'exceptions associée, aussi appelée liste « Do Not Block (Ne pas bloquer) ». Le seul objet de la liste d'exceptions est d'exempter les adresses IP ou les URL qui apparaissent dans la liste de blocage. Autrement dit, si vous trouvez une adresse ou une URL que vous devez utiliser et dont vous savez qu'elle est sûre, mais qu'elle figure dans un flux configuré dans la liste de blocage, vous pouvez exempter ce réseau/cette URL sans retirer complètement la catégorie de la liste de blocage.

Le trafic exempté est ensuite évalué par la stratégie de contrôle d'accès. La décision finale sur l'autorisation ou l'abandon des connexions dépend de la règle de contrôle d'accès à laquelle les connexions correspondent. La règle d'accès détermine également si une inspection de prévention des intrusions ou de programmes malveillants est appliquée à la connexion.

Catégories de flux de renseignements sur la sécurité

Le tableau suivant décrit les catégories disponibles dans les flux Cisco Talos Intelligence Group (Talos). Ces catégories sont disponibles à la fois pour le blocage de réseau et d'URL.

Ces catégories peuvent changer au fil du temps, de sorte qu'un flux nouvellement téléchargé peut comporter des changements de catégorie. Lors de la configuration des renseignements sur la sécurité, vous pouvez cliquer sur l'icône d'information à côté d'un nom de catégorie pour afficher une description.

Tableau 11 : Catégories de flux Cisco Talos Intelligence Group (Talos)

Catégorie de renseignements sur la sécurité	Description
Agresseurs	Analyseurs et hôtes actifs connus pour les activités malveillantes sortantes
fraude_bancaire	Sites qui se livrent à des activités frauduleuses liées aux services bancaires électroniques
bogon	Réseaux de bogons et adresses IP non attribuées
Robots logiciels	Sites qui hébergent des pipettes de programmes malveillants binaires
CNC	Sites qui hébergent des serveurs de commande et de contrôle pour les réseaux de zombies
Cryptominage	Hôtes fournissant un accès à distance aux ensembles et aux portefeuilles dans le but d'exploiter des crypto-devises

Catégorie de renseignements sur la sécurité	Description
Dga	Algorithmes de programmes malveillants utilisés pour générer un grand nombre de noms de domaine agissant comme points de rendez-vous avec leurs serveurs de commande et de contrôle
Kit d'exploit	Trousses de logiciels conçues pour identifier les vulnérabilités des logiciels des clients.
Risque_élevé	Les domaines et les noms d'hôte qui correspondent aux algorithmes de sécurité prédictive OpenDNS du graphique de sécurité
Ioc	Hôtes qui ont été observés en train de s'engager dans les indicateurs de compromission (IOC)
partage_de_liens	Sites Web qui partagent des fichiers protégés par des droits d'auteur sans autorisation
Malveillant	Sites ayant un comportement malveillant qui ne correspondent pas nécessairement à une autre catégorie de menace, plus précise,
Maliciels	Sites qui hébergent des fichiers binaires ou des kits d'exploit de programmes malveillants
Nouvellement_vu	Les domaines qui ont été récemment enregistrés ou qui ne sont pas encore vus par télémétrie. **Attention** Actuellement, cette catégorie ne comporte aucun flux actif et est réservée pour une utilisation future.
Mandataires_ouverts	Des mandataires ouverts qui permettent la navigation anonyme sur le Web
Relais_ouvert	Ouvrir les relais de messagerie connus pour être utilisés pour les pourriels
Hameçonnage	Les sites qui hébergent des pages d'hameçonnage
Intervention	Adresses IP et URL qui participent activement à des activités malveillantes ou suspectes
Pourriels	Hôtes de messagerie connus pour envoyer des pourriels
Logiciel espion	Sites connus pour contenir, diffuser ou soutenir des activités de logiciels espions et publicitaires
Suspect	Fichiers qui semblent suspects et dont les caractéristiques ressemblent à celles d'un logiciel malveillant connu
nœud_exit_de_tor	Hôtes connus pour offrir des services de nœud de sortie pour le réseau d'anonymisation Tor

Exigences de licence pour les renseignements sur la sécurité

Vous devez activer la licence **Menace** pour utiliser Security Intelligence. Consultez Activation ou désactivation des licences facultatives, à la page 95.

Configurer les renseignements sur la sécurité

La politique de renseignements sur la sécurité vous donne l'occasion d'abandonner rapidement le trafic indésirable en fonction de l'adresse IP source/de destination ou de l'URL de destination. Les connexions autorisées sont toujours évaluées par les politiques de contrôle d'accès et sont susceptibles d'être interrompues. Vous devez activer les licences et Threat license (licence Threat) pour pouvoir utiliser Security Intelligence.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **Security Intelligence**.

Étape 2 Si la politique n'est pas activée, cliquez sur le bouton **Enable Security Intelligence** (Activer Security Intelligence).

Vous pouvez désactiver la politique à tout moment en cliquant sur le commutateur **Security Intelligence** pour le mettre sur **Off** (Désactivé). Votre configuration est conservée, de sorte que lorsque vous réactivez la politique, vous n'avez pas besoin de la reconfigurer.

Étape 3 Configurer Security Intelligence.

Il existe des listes de blocage distinctes pour les réseaux (adresses IP) et les URL.

a) Cliquez sur l'onglet **Network** (Réseau) ou **URL** pour afficher la liste que vous souhaitez configurer.

b) Dans la liste de blocage/abandon, cliquez sur **+** pour sélectionner les objets ou les flux dont vous souhaitez abandonner immédiatement les connexions.

Le sélecteur d'objet organise les objets et les flux sur des onglets distincts par type. Si l'objet que vous souhaitez n'existe pas encore, cliquez sur le lien **Create New Object** (Créer un nouvel objet) en bas de la liste et créez-le maintenant. Pour une description des flux Cisco Talos Intelligence Group (Talos), cliquez sur le bouton **i** à côté du flux. Consultez aussi Catégories de flux de renseignements sur la sécurité, à la page 492.

Remarque
Security Intelligence ignore les blocs d'adresses IP utilisant un masque de réseau /0. Cela inclut les objets réseau any-ipv4 et any-ipv6. Ne sélectionnez pas ces objets pour le blocage réseau.

c) Dans la liste Do Not Block (Ne pas bloquer), cliquez sur **+** et sélectionnez les exceptions à la liste de blocage.

La seule raison de configurer cette liste est de faire des exceptions pour les adresses IP ou les URL qui se trouvent dans la liste de blocage. Les connexions exemptées sont ensuite évaluées par votre politique de contrôle d'accès et peuvent être abandonnées de toute façon.

d) Répétez le processus pour configurer l'autre liste de blocage.

Étape 4 (Facultatif) Cliquez sur le bouton **Edit Logging Settings** (Paramètres de journalisation) ( ) pour configurer la journalisation.

Si vous activez la journalisation, toutes les correspondances avec les entrées de liste bloquées sont enregistrées. Les correspondances avec les entrées d'exceptions ne sont pas journalisées, bien que vous obteniez des messages de journalisation si les connexions exemptées correspondent aux règles de contrôle d'accès avec la journalisation activée.

Configurez les paramètres suivants :

- **Connection Events Logging** (Journalisation des événements de connexion) : cliquez sur la bascule pour activer ou désactiver la journalisation.
- **Syslog** : si vous souhaitez envoyer une copie des événements à un serveur syslog externe, sélectionnez cette option et sélectionnez l'objet serveur qui définit le serveur syslog. Si l'objet requis n'existe pas déjà, cliquez sur **Add Syslog Server** (Ajouter un serveur syslog) et créez-le.

  Comme le stockage d'événements sur l'appareil est limité, l'envoi des événements à un serveur journal système externe peut fournir un stockage à plus long terme et améliorer votre analyse des événements.

Surveillance de l'intelligence de sécurité

Si vous activez la journalisation pour la politique Security Intelligence, le système génère des événements Security Intelligence pour chaque connexion qui correspond à un élément d'une liste de blocage. Les événements de connexion correspondent à ces connexions.

Les statistiques pour les connexions abandonnées s'affichent dans les différents tableaux de bord disponibles sur la page Surveillance.

Le tableau de bord **Monitoring (Surveillance)** > **Access And SI Rules (Règles d'accès et SI)** affiche les principales règles d'accès et les règles Security Intelligence équivalentes qui correspondent au trafic.

En outre, vous pouvez sélectionner **Monitoring (Surveillance)** > **Events (Événements**, puis l'affichage **Security Intelligence (Security Intelligence)**, pour voir les événements Security Intelligence, ainsi que les événements de connexion associés sous l'onglet **Connection (Connexion)**.

- Le champ SI Category ID (ID de catégorie SI) dans un événement indique l'objet mis en correspondance dans la liste de blocage, par exemple un objet ou un flux de réseau ou d'URL.
- Le champ Reason (Raison) d'un événement de connexion explique pourquoi l'action affichée dans l'événement a été appliquée. Par exemple, une action Block (Blocage) associée à des raisons telles que IP Block (Blocage IP) ou URL Block (Blocage d'URL) indique qu'une connexion a été abandonnée par Security Intelligence.

Exemples pour les renseignements sur la sécurité

Le chapitre de cas d'utilisation comprend un exemple de mise en œuvre des politiques de sécurité Security Intelligence. Veuillez consulter Comment bloquer les menaces, à la page 56.



CHAPITRE 21

Contrôle d'accès

Les rubriques suivantes expliquent comment gérer les règles de contrôle d'accès. Ces règles contrôlent le trafic autorisé à passer par le périphérique et appliquent des services avancés au trafic, comme l'inspection de prévention des intrusions.

- Bonnes pratiques pour les règles de contrôle d'accès, à la page 497
- Aperçu du contrôle d'accès, à la page 500
- Exigences de licence pour le contrôle d'accès, à la page 512
- Lignes directrices et limites pour les stratégies de contrôle d'accès, à la page 513
- Configuration de la politique de contrôle d'accès, à la page 515
- Gestion des stratégies de contrôle d'accès, à la page 529
- Exemples pour le contrôle d'accès, à la page 531

Bonnes pratiques pour les règles de contrôle d'accès

La politique de contrôle d'accès est votre outil principal pour protéger vos réseaux internes et empêcher vos utilisateurs d'accéder à des ressources de réseau externes indésirables, comme les sites Web inappropriés. Ainsi, nous vous recommandons d'accorder une attention particulière à cette politique et de l'affiner pour obtenir le niveau de protection et de connectivité dont vous avez besoin.

La procédure suivante fournit un aperçu des éléments de base que vous devez faire avec la politique de contrôle d'accès. Il s'agit d'un aperçu et ne fournit pas d'étapes exhaustives pour effectuer chaque tâche.

Pour accéder à la politique de contrôle d'accès, choisissez **Policies (Politiques)** > **Access Control (Contrôle d'accès)**.

Procédure

Étape 1 Configurez l'action par défaut pour la politique.

L'action par défaut gère les connexions qui ne correspondent pas aux règles spécifiques de la politique. Par défaut, cette action est **Block** (Bloquer), de sorte que tout ce que vous manquez dans les règles est bloqué. Ainsi, il vous suffit d'écrire des règles de contrôle d'accès qui autorisent le trafic souhaité. Il s'agit de la façon traditionnelle de configurer la politique de contrôle d'accès.

Vous pouvez faire le contraire, où vous autorisez le trafic par défaut et écrivez des règles qui suppriment le trafic indésirable connu, de sorte que vous n'avez pas besoin d'avoir des règles pour tout ce que vous souhaitez

autoriser. Cela facilite l'utilisation des nouveaux services, mais ouvre le risque que le nouveau trafic indésirable passe avant que vous ne le remarquiez.

Étape 2 Cliquez sur le bouton **Access Policy Settings** (Paramètres de la politique d'accès) ( ) et activez l'option **TLS Server Identity Discovery**.

Cette option améliore la détection initiale de l'application et l'identification de la catégorie d'URL et de la réputation pour les connexions TLS 1.3. Si vous n'activez pas cette option, le trafic TLS 1.3 pourrait ne pas correspondre aux règles que vous souhaitez. Cette option peut également améliorer l'efficacité des règles de déchiffrement.

Étape 3 Créez aussi peu de règles de contrôle d'accès que possible.

Avec les pare-feu traditionnels, vous pourriez vous retrouver avec des dizaines de milliers de règles pour diverses combinaisons d'adresse IP et de port. Avec un pare-feu de nouvelle génération, vous pouvez utiliser l'inspection avancée et éviter certaines de ces règles détaillées. Moins vous avez de règles, plus rapide le système peut évaluer le trafic et plus il sera facile pour vous de détecter et de résoudre les problèmes dans votre ensemble de règles.

Étape 4 Activation de la journalisation pour vos règles de contrôle d'accès.

Les statistiques sont collectées pour le trafic correspondant uniquement si vous activez la journalisation. Vos tableaux de bord de surveillance seront inexacts si vous n'activez pas la journalisation.

Étape 5 Placez des règles très spécifiques en haut de la politique, et assurez-vous que les règles spécifiques sont supérieures à toute règle plus générale qui correspondrait aux connexions auxquelles une règle spécifique correspondrait également.

La politique est évaluée de haut en bas, la première correspondance l'emporte. Ainsi, si vous mettez dans une règle qui bloque tout le trafic vers un sous-réseau spécifique, puis suivez-la avec une règle qui permet l'accès à une adresse IP unique dans le sous-réseau, le trafic vers cette adresse ne sera pas autorisé, car la première règle le bloquera.

En outre, placez des règles qui ciblent le trafic en fonction uniquement des critères classiques, tels que l'interface d'entrée/sortie, l'adresse IP source/destination, le port ou la géolocalisation, avant les règles qui nécessitent une inspection approfondie, comme celles qui s'appliquent aux critères de l'utilisateur, au filtrage d'URL ou au filtrage d'application. Étant donné que ces règles ne nécessitent pas d'inspection, leur application précoce peut vous aider à prendre des décisions de contrôle d'accès plus rapides pour les connexions correspondantes.

Pour plus de suggestions, consultez Bonnes pratiques pour l'ordre des règles de contrôle d'accès, à la page 511.

Étape 6 Associez les règles de blocage et d'autorisation pour cibler des sous-ensembles de trafic.

Par exemple, il est possible que vous souhaitiez autoriser un volume important de trafic HTTP/HTTPS, tout en bloquant l'accès à certains sites indésirables, comme la pornographie ou les jeux d'argent. Vous pouvez le faire en créant les règles suivantes et en les gardant séquentielles dans la politique (par exemple, règles 11 et 12).

- Une règle de blocage de filtrage d'URL qui cible les catégories d'URL indésirables, appliquée à la zone de sécurité interne (source) et à la zone de sécurité externe (destination), et toute adresse IP, tout port ou géolocalisation. Par exemple, blocage des réseaux de zombies, contenu maltraitant envers les enfants, cryptojacking, tunnellisation DNS, fraude bancaire en ligne, exploits, évitement de filtre, jeux d'argent, piratage, discours de haine, sites et emplacements à haut risque, activités illégales, téléchargements illégaux, drogues illégales, sites malveillants, sites de programmes malveillants, menaces mobiles, nœud de programmes malveillants P2P, hameçonnage, pornographie, pourriels, logiciels espions et logiciels publicitaires.

- Une règle d'autorisation de filtrage d'application pour les applications HTTP et HTTPS, appliquée à la zone de sécurité interne (source) et à la zone de sécurité externe (destination), et toute adresse IP, tout port ou géolocalisation. Une fois que la règle de filtrage d'URL a bloqué l'accès aux ressources Web indésirables, cette règle autorise tous les autres accès HTTP/HTTPS.

Étape 7 Utilisez les fonctionnalités de pare-feu de nouvelle génération pour cibler le trafic, quels que soient l'adresse IP ou le port.

Les agresseurs ou d'autres personnes malveillantes peuvent fréquemment modifier les adresses IP et les ports pour contourner les critères de correspondance du trafic de contrôle d'accès traditionnel. Au lieu de cela, utilisez les fonctionnalités de nouvelle génération suivantes :

- Critères de l'utilisateur : configurez la politique d'identité pour obtenir des informations sur l'utilisateur qui lance le trafic. Idéalement, votre serveur Active Directory organise les utilisateurs en groupes, et vous pouvez créer des règles de contrôle d'accès qui autorisent ou bloquent le trafic en fonction de l'appartenance au groupe d'utilisateurs. Par exemple, autorisez les spécialistes en ingénierie à accéder à vos sous-réseaux de développement, mais bloquez implicitement toute personne qui ne fait pas partie du groupe des spécialistes en ingénierie. Utilisez des groupes plutôt que des noms d'utilisateurs individuels, de sorte que vous n'avez pas besoin de mettre à jour continuellement les règles à mesure que des personnes sont ajoutées au réseau.
- Critères d'application : utilisez les critères de filtrage d'application pour autoriser ou bloquer les types d'application. Ainsi, si un utilisateur modifie les ports pour une connexion HTTP, le système peut reconnaître qu'il s'agit d'une connexion HTTP, même s'il ne va pas au port 80. Pour plus de suggestions, consultez Bonnes pratiques pour le filtrage d'applications, à la page 502.
- Catégorie d'URL et critères de réputation : utilisez le filtrage d'URL basé sur la catégorie pour autoriser ou bloquer dynamiquement les sites en fonction du type de site. Dans le type ou la catégorie du site, vous pouvez affiner votre règle selon que le site a la réputation d'être bon ou mauvais acteur. En utilisant la catégorie et la réputation, vous n'aurez pas besoin d'ajuster constamment vos règles, car les sites changent d'URL, ce que vous devriez faire si vous avez essayé de bloquer manuellement les sites par URL. Pour plus de suggestions, consultez Bonnes pratiques pour un filtrage d'URL efficace, à la page 507.

  Vous pouvez également appliquer vos règles de catégorie et de réputation de filtrage d'URL aux demandes de consultation DNS. Le système peut empêcher la réponse DNS pour la catégorie bloquée/la réputation, bloquant efficacement la tentative de connexion de l'utilisateur. Pour de plus amples renseignements, consultez la section Filtrage des requêtes DNS en fonction de la catégorie d'URL et de la réputation, à la page 510.

Étape 8 Appliquez l'inspection des intrusions à toutes vos règles d'autorisation.

L'un des aspects les plus importants des pare-feu de nouvelle génération est que vous pouvez appliquer l'inspection des intrusions et le contrôle d'accès à l'aide du même périphérique. Appliquez une politique de prévention des intrusions à chaque règle d'autorisation, de sorte que si une attaque entre dans votre réseau par un chemin normalement inoffensif, vous puissiez la détecter et abandonner la connexion d'attaque.

Si votre action par défaut est Allow (autoriser), vous pouvez également appliquer une protection contre les intrusions pour le trafic qui correspond à l'action par défaut.

Étape 9 Configurez également la Security Intelligence policy (politique Security Intelligence) pour bloquer les adresses IP et les URL indésirables.

La politique Security Intelligence est appliquée avant la politique de contrôle d'accès, de sorte qu'elle peut bloquer les connexions indésirables avant que vos règles de contrôle d'accès ne soient même évaluées. Cela peut fournir un blocage précoce et vous aider à réduire la complexité de vos règles de contrôle d'accès.

Étape 10 Envisagez de mettre en œuvre la SSL Decryption policy (politique de déchiffrement SSL).

Le système n'effectue pas d'inspection approfondie du trafic chiffré. Si vous configurez la politique de déchiffrement SSL, la politique de contrôle d'accès est appliquée à une version déchiffrée du trafic. Ainsi, l'inspection approfondie peut identifier les attaques (à l'aide de la politique de prévention des intrusions) et la mise en correspondance des règles est meilleure, car le filtrage des applications et des URL peut être appliqué plus efficacement. Tout trafic autorisé par la politique de contrôle d'accès est ensuite rechiffré avant d'être envoyé par le périphérique, de sorte que l'utilisateur final ne perd pas la protection du chiffrement.

Étape 11 Activez la recherche de groupe d'objets pour simplifier le déploiement de vos règles.

L'activation de la recherche de groupe d'objets réduit les besoins en mémoire pour les stratégies de contrôle d'accès qui incluent des objets réseau. Cependant, il est important de noter que la recherche par groupe d'objets peut également diminuer les performances de la recherche de règles et donc augmenter l'utilisation de l'unité centrale. Vous devez équilibrer l'incidence sur le processeur et le besoin en mémoire réduits pour la stratégie de contrôle d'accès spécifique. Dans la plupart des cas, l'activation de la recherche de groupe d'objets offre une nette amélioration opérationnelle.

Vous pouvez définir cette option à l'aide de FlexConfig en envoyant la commande **object-group-search access-control** ; utilisez la forme **no** de la commande dans le modèle de négation.

Aperçu du contrôle d'accès

Les rubriques suivantes expliquent comment gérer les règles de contrôle d'accès.

Règles de contrôle d'accès et action par défaut

Utilisez la politique de contrôle d'accès pour autoriser ou bloquer l'accès aux ressources réseau. La politique consiste en un ensemble de règles ordonnées, qui sont évaluées de haut en bas. La règle appliquée au trafic est la première s'appliquant, entraînant la mise en correspondance de tous les critères de trafic.

Vous pouvez contrôler l'accès en fonction des éléments suivants :

- Caractéristiques du réseau traditionnelles telles que les adresses IP source et de destination, le protocole, les ports et les interfaces (sous forme de zones de sécurité).
- Le nom de domaine complet (FQDN) de la source ou de la destination (sous forme d'objet réseau). La correspondance du trafic est basée sur l'adresse IP renvoyée pour le nom d'une recherche DNS.
- La balise de groupe de sécurité (SGT) attribuée à la source ou à la destination par le Cisco Identity Services Engine (ISE).
- L'application qui est utilisée. Vous pouvez contrôler l'accès en fonction de l'application spécifique ou vous pouvez créer des règles qui couvrent les catégories d'applications, les applications marquées d'une caractéristique particulière, le type d'application (client, serveur, Web) ou l'évaluation de risque ou de pertinence commerciale de l'application.
- L'URL de destination d'une demande Web, y compris la catégorie généralisée de l'URL. Vous pouvez affiner les correspondances de catégorie en fonction de la réputation publique du site cible.

- La catégorie d'URL et la réputation d'un FQDN dans une demande de recherche DNS. Vous pouvez bloquer la réponse DNS pour les catégories indésirables ou pour mauvaise réputation, ce qui empêche efficacement la tentative de connexion ultérieure.
- L'utilisateur qui fait la demande ou les groupes d'utilisateurs auxquels l'utilisateur appartient.

Pour le trafic non chiffré que vous autorisez, vous pouvez appliquer l'inspection IPS pour vérifier les menaces et bloquer le trafic qui semble être une attaque. Vous pouvez également utiliser des politiques de fichiers pour vérifier les fichiers interdits ou les programmes malveillants.

Tout trafic qui ne correspond à aucune règle de contrôle d'accès est géré par l'action par défaut de contrôle d'accès **Default Action** (Action par défaut). Si vous autorisez le trafic par défaut, vous pouvez appliquer l'inspection de prévention des intrusions au trafic. Cependant, vous ne pouvez pas inspecter les fichiers ou les programmes malveillants sur le trafic géré par l'action par défaut.

Filtrage d'applications

Vous pouvez utiliser des règles de contrôle d'accès pour filtrer le trafic en fonction de l'application utilisée dans la connexion. Le système peut reconnaître une grande variété d'applications, de sorte que vous n'avez pas besoin de comprendre comment bloquer une application Web sans bloquer toutes les applications Web.

Pour certaines applications populaires, vous pouvez filtrer selon différents aspects de l'application. Par exemple, vous pourriez créer une règle qui bloque les jeux Facebook sans bloquer tout Facebook.

Vous pouvez également créer des règles en fonction des caractéristiques générales des applications, en bloquant ou en autorisant des groupes entiers d'applications selon le risque ou la pertinence métier, le type, la catégorie ou la balise. **Toutefois, lorsque vous sélectionnez des catégories dans un filtre d'application, consultez la liste des applications correspondantes pour vous assurer de ne pas inclure d'applications non souhaitées.** Pour une explication détaillée des regroupements possibles, consultez Critères d'application, à la page 521.

Application Control pour le trafic chiffré et déchiffré

Si une application utilise le chiffrement, le système pourrait ne pas être en mesure d'identifier l'application.

Le système peut détecter le trafic d'applications chiffré avec StartTLS, y compris SMTPS, POPS, FTPS, TelnetS et IMAPS. En outre, il peut identifier certaines applications chiffrées en fonction de l'indication du nom du serveur dans le message TLS ClientHello ou de la valeur du nom distinctif du sujet provenant du certificat du serveur.

Utilisez la boîte de dialogue Application Filters (Filtres d'application) pour déterminer si votre application nécessite un déchiffrement : sélectionnez les Tags (Balises) suivants, puis examinez la liste des applications.

- **SSL Protocol** (Protocole SSL) : vous n'avez pas besoin de déchiffrer le trafic associé à la balise SSL Protocol. Le système peut reconnaître ce trafic et appliquer votre action de contrôle d'accès. Les règles de contrôle d'accès pour les applications répertoriées doivent correspondre aux connexions attendues.
- **Decrypted Traffic** (Trafic déchiffré) : le système ne peut reconnaître ce trafic que si vous le déchiffrez d'abord. Configurez des règles de déchiffrement SSL pour ce trafic.

Filtrage en fonction du protocole industriel commun (CIP) et des applications Modbus (ISA 3000)

Vous pouvez activer le protocole industriel commun (CIP) et les préprocesseurs Modbus sur les périphériques Cisco ISA 3000, et filtrer en fonction des applications CIP et Modbus dans les règles de contrôle d'accès.

Tous les noms d'applications CIP commencent par « CIP », tel que CIP Write. Il n'y a qu'une seule application pour Modbus.

Pour activer les préprocesseurs, vous devez passer en mode expert dans une session CLI (SSH ou console) et exécuter la commande suivante pour activer l'une ou les deux applications de contrôle de supervision et d'acquisition de données (SCADA).

sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}

Par exemple, pour activer les deux préprocesseurs :

```
> expert
admin@firepower:~$ sudo /usr/local/sf/bin/enable_scada.sh both
```



Remarque Vous devez exécuter cette commande après chaque déploiement. Ces préprocesseurs sont désactivés lors du déploiement.

Bonnes pratiques pour le filtrage d'applications

Veuillez garder les recommandations suivantes à l'esprit lors de la conception des règles de contrôle d'accès de filtrage d'application.

- Pour gérer le trafic référencé par un serveur Web, tel que le trafic publicitaire, faites correspondre l'application référencée plutôt que l'application de référence.
- Évitez de combiner les critères d'application et d'URL dans la même règle, en particulier pour le trafic chiffré.
- Si vous écrivez une règle pour un trafic étiqueté **Decrypted Traffic** (Trafic déchiffré), assurez-vous de disposer d'une règle SSL Decryption (Déchiffrement SSL) qui déchiffrera le trafic correspondant. Ces applications ne peuvent être identifiées que dans les connexions déchiffrées.
- TLS 1.3 chiffre la plupart des messages d'établissement de liaison, de sorte que les renseignements sur les certificats ne sont pas facilement accessibles. Pour que le trafic chiffré avec TLS 1.3 corresponde efficacement aux règles d'accès qui utilisent le filtrage d'applications ou d'URL, le système doit obtenir un certificat en clair pour le serveur. Nous vous recommandons d'activer **TLS 1.3 Certificate Visibility (visibilité des certificats TLS 1.3)** dans les paramètres de contrôle d'accès. Si vous activez cette option, le système vérifie si un certificat pour le site est stocké en cache en fonction de l'adresse IP et de l'indication du nom du serveur (SNI) dans le paquet client « hello » Si aucun certificat n'est disponible, le système utilise une sonde TLS 1.2 pour obtenir le certificat, qui pourra ensuite être utilisé pour identifier la catégorie et la réputation de l'application ou de l'URL sans déchiffrer la connexion.
- Le système peut détecter plusieurs types de trafic d'application Skype. Pour contrôler le trafic Skype, choisissez la balise Skype dans la liste Application Filters (Filtres d'application) plutôt que de sélectionner des applications individuelles. Cela garantit que le système peut détecter et contrôler tout le trafic de Skype de la même manière.
- Pour contrôler l'accès à la messagerie Zoho, sélectionnez les applications Zoho et Zoho Mail.

Filtrage URL

Vous pouvez utiliser des règles de contrôle d'accès pour filtrer le trafic en fonction de l'URL utilisée dans une connexion HTTP ou HTTPS. Notez que le filtrage d'URL pour HTTP est plus simple que pour HTTPS, car HTTPS est chiffré.

Vous pouvez utiliser les techniques suivantes pour mettre en œuvre le filtrage d'URL.

- Filtrage d'URL basé sur la catégorie et la réputation : avec une licence de filtrage d'URL, vous pouvez contrôler l'accès aux sites Web en fonction de la classification générale de l'URL (catégorie) et du niveau de risque (réputation). Il s'agit de loin du moyen le plus simple et le plus efficace pour bloquer les sites indésirables.
- Filtrage manuel d'URL : avec n'importe quelle licence, vous pouvez spécifier manuellement des URL individuelles et des groupes d'URL afin d'obtenir un contrôle granulaire et personnalisé du trafic Web. L'objectif principal du filtrage manuel est de créer des exceptions aux règles de blocage basées sur une catégorie, mais vous pouvez utiliser des règles manuelles à d'autres fins.

Les rubriques suivantes fournissent des informations supplémentaires sur le filtrage d'URL.

Filtrage des URL par catégorie et par réputation

Avec une licence de filtrage d'URL, vous pouvez contrôler l'accès aux sites Web en fonction de la catégorie et de la réputation des URL demandées :

- Catégorie : classification générale pour l'URL. Par exemple, eBay.com appartient à la catégorie Enchères et monster.com appartient à la catégorie Recherche d'emploi. Une URL peut appartenir à plusieurs catégories.
- Réputation : la probabilité que l'URL soit utilisée à des fins contraires à la politique de sécurité de votre organisation. Les réputations s'échelonnent de Non fiable (niveau 1) à Fiable (niveau 5). La réputation est déterminée par le nom de domaine. Par exemple, toutes les pages du site www.cisco.com sont considérées comme ayant la même réputation.

Les catégories d'URL et les réputations vous aident à configurer rapidement le filtrage d'URL. Par exemple, vous pouvez utiliser le contrôle d'accès pour bloquer les URL non fiables dans la catégorie Drogues illégales.

Pour une description des catégories, consultez https://www.talosintelligence.com/categories.

L'utilisation des données de catégorie et de réputation simplifie également la création et l'administration des politiques. Des sites qui (par exemple) représentent des menaces pour la sécurité ou qui diffusent du contenu indésirable peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer de nouvelles politiques. Lorsque Cisco met à jour la base de données d'URL avec de nouveaux sites, des classifications modifiées et des réputations modifiées, vos règles s'ajustent automatiquement aux nouvelles informations. Vous n'avez pas besoin de modifier vos règles pour prendre en compte les nouveaux sites.

Si vous activez les mises à jour régulières de la base de données d'URL, vous pouvez vous assurer que le système utilise des informations à jour pour le filtrage d'URL. Vous pouvez également activer les communications avec Cisco Collective Security Intelligence (CSI) pour obtenir les dernières informations sur les menaces pour les URL de catégorie et de réputation inconnues. Pour en savoir plus, consultez Configuration des préférences de filtrage Cloud , à la page 814.



Remarque Pour voir les informations de catégorie d'URL et de réputation dans les événements et les détails de l'application, vous devez créer au moins une règle avec une condition d'URL.

Recherche de la catégorie et de la réputation d'une URL

Vous pouvez vérifier la catégorie et la réputation d'une URL particulière. Vous pouvez accéder à l'onglet URL d'une règle de contrôle d'accès ou d'une règle de déchiffrement SSL, ou encore aller à **Device (Périphérique)** > **System Settings (Paramètres système)** > **URL Filtering Preferences (Préférences de filtrage d'URL)**. Vous pouvez y saisir l'URL dans le champ **URL to Check** (URL à vérifier) et cliquer sur **Go** (Aller).

Vous serez redirigé vers un site Web qui affiche les résultats de la recherche. Vous pouvez utiliser ces renseignements pour vous aider à vérifier le comportement de vos règles de filtrage d'URL basées sur la catégorie et la réputation.

Si vous êtes en désaccord avec la catégorisation, vous pouvez cliquer sur **Submit a URL Category Dispute** (Soumettre une contestation de catégorie d'URL) dans le Gestionnaire de périphériques de pare-feu pour nous faire savoir ce que vous pensez.

Filtrage manuel des URL

Vous pouvez compléter ou remplacer de manière sélective le filtrage d'URL basé sur la catégorie et la réputation en filtrant manuellement des URL individuelles ou des groupes d'URL. Vous pouvez effectuer ce type de filtrage d'URL sans licence spéciale.

Par exemple, vous pourriez utiliser le contrôle d'accès pour bloquer une catégorie de sites Web qui ne conviennent pas à votre organisation. Toutefois, si la catégorie contient un site Web approprié et auquel vous souhaitez fournir l'accès, vous pouvez créer une règle Allow (Autoriser) manuelle pour ce site et la placer avant la règle Block (Bloquer) de la catégorie concernée.

Pour configurer le filtrage d'URL manuel, vous créez un objet URL avec l'URL de destination. La façon dont cette URL est interprétée dépend des règles suivantes :

- Si vous n'incluez pas de chemin (c'est-à-dire qu'il n'y a pas de caractères / dans l'URL), la correspondance est basée sur le nom d'hôte du serveur uniquement. Si vous incluez un ou plusieurs caractères /, la chaîne URL complète est utilisée pour une correspondance de sous-chaîne. Ainsi, une URL est considérée comme en correspondance si l'une des conditions suivantes est remplie :
  - La chaîne se trouve au début de l'URL.
  - La chaîne suit un point.
  - La chaîne contient un point au début.
  - La chaîne suit les caractères ://.

  Par exemple, ign.com correspond à ign.com ou www.ign.com, mais pas à versign.com.

Remarque Nous vous recommandons de ne pas utiliser le filtrage manuel d'URL pour bloquer ou autoriser des pages Web individuelles ou des parties de sites (c'est-à-dire les chaînes URL avec des caractères /), car les serveurs peuvent être réorganisés et les pages déplacées vers de nouveaux chemins.

- Le système ne tient pas compte du protocole de chiffrement (HTTP ou HTTPS). En d'autres termes, si vous bloquez un site Web, les trafics HTTP et HTTPS vers ce site Web sont bloqués, sauf si vous utilisez une condition d'application pour cibler un protocole spécifique. Lors de la création d'un objet URL, vous n'avez pas besoin de préciser le protocole lors de la création d'un objet. Par exemple, utilisez exemple.com plutôt que http://exemple.com.
- Si vous prévoyez utiliser un objet URL pour faire correspondre le trafic HTTPS dans une règle de contrôle d'accès, créez l'objet en utilisant le nom usuel du sujet dans le certificat de clé publique utilisé pour chiffrer le trafic. De plus, le système ne tient pas compte des sous-domaines du nom usuel du sujet. N'incluez donc pas les informations de ce sous-domaine. Par exemple, utilisez exemple.com plutôt que www.exemple.com.

  Cependant, veuillez comprendre que le nom usuel du sujet dans le certificat peut être complètement sans rapport avec le nom de domaine d'un site Web. Par exemple, le nom usuel du sujet dans le certificat pour youtube.com est *.Google.com (bien entendu, cela peut changer à tout moment). Vous obtiendrez des résultats plus cohérents si vous utilisez la politique de déchiffrement SSL pour déchiffrer le trafic HTTPS afin que les règles de filtrage d'URL fonctionnent sur le trafic déchiffré.

Remarque Les objets URL ne correspondront pas au trafic HTTPS si le navigateur reprend une session TLS, car les informations de certificat ne sont plus disponibles. Ainsi, même si vous configurez soigneusement l'objet URL, vous pourriez obtenir des résultats incohérents pour les connexions HTTPS.

Filtrage du trafic HTTPS

Comme le trafic HTTPS est chiffré, effectuer le filtrage d'URL directement sur le trafic HTTPS n'est pas aussi simple que de le faire sur le trafic HTTP. Pour cette raison, vous devez envisager d'utiliser des politiques de déchiffrement SSL pour déchiffrer tout le trafic HTTPS que vous avez l'intention de filtrer. De cette façon, les politiques de contrôle d'accès de filtrage d'URL fonctionnent sur le trafic déchiffré, et vous obtenez les mêmes résultats que vous obtiendriez pour le trafic HTTP normal.

Toutefois, si vous avez l'intention d'autoriser qu'une partie du trafic HTTPS passe non déchiffré dans la politique de contrôle d'accès, vous devez comprendre que les règles font correspondre le trafic HTTPS différemment de ce qu'elles font pour le trafic HTTP. Pour filtrer le trafic chiffré, le système détermine l'URL demandée en fonction des informations transmises lors de la prise de contact SSL : le nom commun du sujet dans le certificat de clé publique utilisé pour chiffrer le trafic. Il peut y avoir peu ou pas de relation entre le nom d'hôte du site Web dans l'URL et le nom commun du sujet.

Vous pouvez améliorer la mise en correspondance HTTPS pour les règles de catégorie/réputation si vous activez le filtrage des demandes DNS. Le système peut déterminer la catégorie et la réputation pendant la phase de résolution DNS et bloquer la réponse DNS pour les combinaisons indésirables, avant que l'utilisateur ne puisse commencer la tentative de connexion HTTPS. Pour les réponses DNS autorisées, le système disposera

des informations de catégorie/réputation disponibles pour les connexions HTTPS ultérieures. Consultez Filtrage des requêtes DNS, à la page 509.

Le filtrage HTTPS, contrairement au filtrage HTTP, ne prend pas en compte les sous-domaines du nom commun du sujet. N'incluez pas d'informations de sous-domaine lors du filtrage manuel des URL HTTPS. Par exemple, utilisez exemple.com plutôt que www.exemple.com. Passez également en revue le contenu des certificats utilisés par le site pour vous assurer que vous avez le bon domaine, celui utilisé dans le nom commun du sujet, et que ce nom n'entrera pas en conflit avec vos autres règles (par exemple, le nom d'un site que vous souhaitez bloquer peut se chevaucher avec un que vous souhaitez autoriser). Par exemple, le nom usuel du sujet dans le certificat pour youtube.com est *.Google.com (bien entendu, cela peut changer à tout moment).

Remarque Les objets URL ne correspondront pas au trafic HTTPS si le navigateur reprend une session TLS, car les informations de certificat ne sont plus disponibles. Ainsi, même si vous configurez soigneusement l'objet URL, vous pourriez obtenir des résultats incohérents pour les connexions HTTPS.

Contrôle du trafic par le protocole de chiffrement

Le système ne tient pas compte du protocole de chiffrement (HTTP ou HTTPS) lors du filtrage d'URL. Cela se produit pour les conditions d'URL manuelles et basées sur la réputation. Autrement dit, le filtrage d'URL traite le trafic vers les sites Web suivants de manière identique :

- http://example.com
- https://example.com

Pour configurer une règle qui correspond uniquement au trafic HTTP ou HTTPS, mais pas aux deux, spécifiez soit le port TCP dans la condition de destination, soit ajoutez une condition d'application à la règle. Par exemple, vous pourriez autoriser l'accès HTTPS à un site tout en interdisant l'accès HTTP en créant deux règles de contrôle d'accès, chacune comportant une condition de port TCP, d'application et d'URL.

La première règle autorise le trafic HTTPS vers le site Web :

Action : Allow (Autoriser)
Port TCP ou application : HTTPS (port TCP 443)
URL : example.com

La deuxième règle bloque l'accès HTTP au même site Web :

Action : Bloc (Bloquer)
Port TCP ou application : HTTP (port TCP 80)
URL : example.com

Comparaison du filtrage d'URL et du filtrage d'applications

Les filtrages d'URL et d'application ont des similitudes. Vous devez toutefois les utiliser à des fins très distinctes :

- Le filtrage d'URL est mieux utilisé pour bloquer ou autoriser l'accès à l'ensemble d'un serveur Web. Par exemple, si vous ne souhaitez autoriser aucun type de jeux d'argent sur votre réseau, vous pouvez créer une règle de filtrage d'URL pour bloquer la catégorie Jeux. Avec cette règle, les utilisateurs ne peuvent accéder à aucune page sur aucun serveur Web dans la catégorie.

- Le filtrage des applications est utile pour bloquer des applications spécifiques, quel que soit le site d'hébergement, ou pour bloquer des fonctionnalités spécifiques d'un site Web par ailleurs autorisé. Par exemple, vous pourriez bloquer uniquement l'application Facebook Jeux sans bloquer tout Facebook.

Parce que la combinaison des critères d'application et d'URL peut entraîner des résultats inattendus, en particulier pour le trafic chiffré, il est bon de créer des règles distinctes pour les critères d'URL et d'application. Si vous devez combiner les critères d'application et d'URL dans une seule règle, vous devriez placer ces règles après les règles d'application uniquement ou d'URL uniquement, sauf si la règle application+URL agit comme une exception à une règle plus générale d'application uniquement ou d'URL uniquement. Étant donné que les règles de blocage de filtrage d'URL sont plus larges que le filtrage d'application, vous devez les placer au-dessus des règles d'application uniquement.

Si vous combinez les critères d'application et d'URL, vous devrez peut-être surveiller votre réseau de plus près pour vous assurer de ne pas autoriser l'accès aux sites et aux applications indésirables.

Bonnes pratiques pour un filtrage d'URL efficace

Veuillez garder les recommandations suivantes à l'esprit lorsque vous concevez vos règles de contrôle d'accès avec filtrage d'URL.

- Utilisez, chaque fois que possible, le blocage fondé sur la catégorie et la réputation. Cela garantit que les nouveaux sites sont automatiquement bloqués lorsqu'ils sont ajoutés aux catégories et que le blocage fondé sur la réputation est ajusté si un site devient plus (ou moins) fiable.
- Lorsque vous utilisez la mise en correspondance par catégorie d'URL, notez qu'il existe des cas où la page de connexion d'un site appartient à une catégorie différente de celle du site lui-même. Par exemple, Gmail se trouve dans la catégorie Web-based Email (Courriel Web), alors que la page de connexion se trouve dans la catégorie Search Engines and Portals (Moteurs de recherche et portails). Si vous avez des règles distinctes avec des actions différentes pour ces catégories, vous pourriez obtenir des résultats inattendus.
- Utilisez des objets d'URL pour cibler des sites Web entiers et créer des exceptions aux règles de blocage par catégorie. Autrement dit, pour autoriser des sites précis qui seraient autrement bloqués par une règle de catégorie.
- Si vous souhaitez bloquer manuellement un serveur Web (au moyen d'un objet d'URL), il est beaucoup plus efficace de le faire dans la politique Security Intelligence. La politique Security Intelligence rejette les connexions avant l'évaluation des règles de contrôle d'accès, ce qui permet un blocage plus rapide et plus efficace.
- Pour filtrer au mieux les connexions HTTPS, mettez en œuvre des règles de déchiffrement SSL pour déchiffrer le trafic auquel vous appliquez une règle de contrôle d'accès. Toute connexion HTTPS déchiffrée est traitée comme une connexion HTTP dans la politique de contrôle d'accès, ce qui vous permet d'éviter les limites propres au filtrage HTTPS.
- TLS 1.3 chiffre la plupart des messages d'établissement de liaison, de sorte que les renseignements sur les certificats ne sont pas facilement accessibles. Pour que le trafic chiffré avec TLS 1.3 corresponde efficacement aux règles d'accès qui utilisent le filtrage d'applications ou d'URL, le système doit obtenir un certificat en clair pour le serveur. Nous vous recommandons d'activer **TLS 1.3 Certificate Visibility (visibilité des certificats TLS 1.3)** dans les paramètres de contrôle d'accès. Si vous activez cette option, le système vérifie si un certificat pour le site est stocké en cache en fonction de l'adresse IP et de l'indication du nom du serveur (SNI) dans le paquet client « hello » Si aucun certificat n'est disponible, le système utilise une sonde TLS 1.2 pour obtenir le certificat, qui pourra ensuite être utilisé pour identifier la catégorie et la réputation de l'application ou de l'URL sans déchiffrer la connexion.

- Placez les règles de blocage d'URL avant toute règle de filtrage d'applications, car le filtrage d'URL bloque des serveurs Web entiers, alors que le filtrage d'applications cible une utilisation spécifique de l'application, quel que soit le serveur Web.
- Si vous souhaitez bloquer des sites à haut risque dont la catégorie est inconnue, sélectionnez la catégorie Uncategorized (Non classé) et ajustez le curseur de réputation sur Questionable (Douteux) ou Untrusted (Non fiable).
- Vous pouvez améliorer l'efficacité globale du filtrage d'URL en activant également le filtrage des demandes DNS. Lorsque vous utilisez le filtrage des demandes DNS, le système détermine la catégorie d'URL et la réputation du nom de domaine complet (FQDN) au moment de la recherche DNS, de sorte que l'information est disponible si une demande HTTP/HTTPS ultérieure vise la même destination. De plus, si vous bloquez la catégorie ou la réputation, la tentative de connexion est arrêtée au stade de la demande DNS plutôt qu'au stade de l'établissement de la session Web. Consultez Filtrage des requêtes DNS, à la page 509.

Ce que l'utilisateur voit lorsque vous bloquez des sites Web

Lorsque vous bloquez des sites Web avec des règles de filtrage d'URL, ce que l'utilisateur voit diffère selon que le site est chiffré.

- Connexions HTTP : l'utilisateur voit une page de réponse de blocage par défaut du système au lieu de la page de navigateur normale pour les connexions expirées ou réinitialisées. Cette page doit indiquer clairement que la connexion a été bloquée intentionnellement.
- Connexions HTTPS (chiffrées) : l'utilisateur ne voit pas la page de réponse au blocage par défaut du système. Au lieu de cela, l'utilisateur voit la page par défaut du navigateur pour un échec de connexion sécurisée. Le message d'erreur n'indique pas que le site a été bloqué en raison de la politique. Au lieu de cela, des erreurs peuvent indiquer qu'il n'y a pas d'algorithmes de chiffrement communs. Ce message n'indique pas clairement que la connexion a été bloquée intentionnellement.

En outre, les sites Web peuvent être bloqués par d'autres règles de contrôle d'accès qui ne sont pas explicitement des règles de filtrage d'URL, ou même par l'action par défaut. Par exemple, si vous bloquez des réseaux entiers ou des géolocalisations, tous les sites Web de ce réseau ou de cet emplacement géographique sont également bloqués. Les utilisateurs bloqués par ces règles peuvent ou non obtenir une page de réponse comme décrit dans les limites ci-dessous.

Si vous mettez en œuvre le filtrage d'URL, pensez à expliquer aux utilisateurs finaux ce qu'ils peuvent voir lorsqu'un site est intentionnellement bloqué et les types de sites que vous bloquez. Sinon, ils pourraient passer beaucoup de temps à résoudre les connexions bloquées.

Limites des pages de réponse HTTP

Les pages de réponse HTTP ne s'affichent pas toujours lorsque le système bloque le trafic Web.

- Le système n'affiche pas de page de réponse lorsque le trafic Web est bloqué en raison d'une règle de contrôle d'accès promu (une règle de blocage placée tôt avec uniquement des conditions de réseau simples).
- Le système n'affiche pas de page de réponse lorsque le trafic Web est bloqué avant que le système ait identifié l'URL demandée.
- Le système n'affiche pas de page de réponse pour les connexions chiffrées bloquées par les règles de contrôle d'accès.

Filtrage des requêtes DNS

Vous pouvez appliquer la base de données de catégorie d'URL et de réputation aux demandes de recherche DNS, même pour les tentatives de connexion qui ne sont pas HTTP/HTTPS.

Par exemple, si un utilisateur tente d'établir une connexion FTP avec www.exemple.com, vous pouvez configurer le système pour rechercher la catégorie et la réputation de www.exemple.com lorsqu'il voit la demande de recherche DNS pour ce nom de domaine complet (FQDN). Si votre règle de filtrage DNS/URL pour la catégorie ou la réputation renvoyée est une règle de blocage, le système bloque la réponse DNS. Ainsi, l'utilisateur n'obtient pas d'adresse IP pour le FQDN et sa tentative de connexion échoue.

En activant le filtrage des demandes de recherche DNS, vous pouvez étendre vos règles de filtrage d'URL à des protocoles autres que HTTP/HTTPS, et empêcher les protocoles FTP, TFTP, SCP, ICMP et tout autre protocole d'établir une connexion avec un site que vous bloquez pour l'accès Web. Cela fonctionne tant que l'utilisateur utilise un nom FQDN et nécessite donc une recherche DNS. Si l'utilisateur utilise une adresse IP, il n'y a pas de demande DNS et le blocage des demandes DNS n'est pas possible.

Pour le trafic HTTP/HTTPS, la recherche de catégorie/réputation au moment de la demande DNS peut améliorer les performances du système, car cela peut empêcher la connexion avant la tentative d'établissement de la session Web. Cela peut être particulièrement utile pour HTTPS, qui est chiffré. En refusant au stade de la demande DNS, le système ne voit jamais de connexion HTTPS, et donc vos règles de déchiffrement n'ont pas besoin d'être évaluées, et le système n'a pas besoin d'effectuer la tâche plus difficile de faire correspondre une session chiffrée à la règle de contrôle d'accès appropriée.

Lignes directrices relatives au filtrage des demandes DNS

Gardez les éléments suivants à l'esprit lorsque vous configurez le filtrage de demande DNS :

- Le filtrage de demande DNS fonctionne uniquement sur la session DNS. Si vous autorisez la réponse DNS (c'est-à-dire si l'action de la règle de filtrage d'URL est Allow (Autoriser)), la connexion ultérieure que l'utilisateur établit avec l'adresse IP renvoyée sera évaluée séparément par rapport à vos règles de contrôle d'accès. La connexion peut correspondre à une règle différente et donc être bloquée ou autorisée pour d'autres raisons. Par exemple, si vous autorisez une tentative FTP d'obtenir une adresse IP par une recherche DNS, vous pouvez avoir une autre règle de contrôle d'accès qui interdise les connexions FTP, et la connexion sera finalement bloquée.
- Les demandes de recherche DNS qui correspondent aux règles de contrôle d'accès qui précèdent vos règles de filtrage de demande d'URL/DNS seront autorisées ou bloquées en fonction de la règle de correspondance. La recherche de catégorie/réputation ne sera pas effectuée pour ces connexions.
- Cette fonctionnalité nécessite que vous mettiez en œuvre le filtrage d'URL en fonction de la catégorie ou de la réputation. Vous devez avoir la licence de filtrage d'URL pour ce type de filtrage d'URL. Si vous n'avez aucune règle de filtrage d'URL en fonction de la catégorie/réputation, le filtrage de demande DNS n'est pas pertinent et vous ne devez pas l'activer.
- Les événements de connexion générés par le filtrage DNS incluent les champs suivants, particulièrement utiles : DNS Query (Requête DNS), URL Category (Catégorie d'URL) et URL Reputation (Réputation d'URL). Le champ DNS Query (Requête DNS) affiche le nom de domaine complet (FQDN) de la demande de recherche. Pour les événements de filtrage DNS, le champ URL sera vide.
- Le filtrage des requêtes DNS utilise uniquement la base de données de catégorie et de réputation d'URL. Tous les objets URL ou autres filtrages d'URL manuels définis dans une règle de contrôle d'accès correspondante sont ignorés. Si vous souhaitez mettre en œuvre le blocage de nom DNS manuel, utilisez la politique DNS Security Intelligence.

Filtrage des requêtes DNS en fonction de la catégorie d'URL et de la réputation

La procédure suivante explique comment mettre en œuvre le filtrage des demandes de recherche DNS.

Avant de commencer

Vous devez activer la licence d'URL si elle n'est pas déjà activée.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **Access Control (Contrôle d'accès**.

Étape 2 Si nécessaire, cliquez sur le bouton **Access Policy Settings** (Paramètres de politique d'accès) ( ), sélectionnez l'option **Reputation Enforcement on DNS Traffic** (Application de la réputation sur le trafic DNS), puis cliquez sur **OK**.

Cette option active le filtrage des demandes DNS pour la politique de contrôle d'accès. Cette option est activée par défaut.

Étape 3 Évaluez les règles de filtrage d'URL existantes ou créez-en de nouvelles pour mettre en œuvre le filtrage en fonction de la catégorie d'URL et de la réputation qui s'appliquera également aux requêtes DNS.

Le filtrage d'URL s'applique normalement uniquement au trafic HTTP/HTTPS, il n'y a donc aucune raison de restreindre ces règles en fonction de l'application ou du port. Toutefois, si vous avez ces restrictions, assurez-vous que la règle peut également s'appliquer aux requêtes DNS :

- Dans l'onglet **Source/Destination**, si le champ **Destination Ports** (Ports de destination) comporte **Any** (N'importe quel), aucune modification n'est nécessaire. Si vous avez spécifié des ports, ajoutez **DNS sur UDP** et **DNS sur TCP** à la liste.
- Dans l'onglet **Applications**, si la liste des applications contient simplement **Any** (N'importe quel), aucune modification n'est nécessaire. Si vous avez spécifié des applications ou des filtres d'application, ajoutez l'application **DNS** à la liste ou au filtre. Les autres options liées au DNS ne sont pas pertinentes dans ce contexte.

Pour plus d'informations sur les règles de contrôle d'accès, consultez Configuration des règles de contrôle d'accès, à la page 517.

Étape 4 Évaluez les règles précédentes pour vous assurer que les requêtes DNS ne correspondent pas à ces règles.

La détermination de la catégorie et de la réputation se produit uniquement si la demande DNS correspond à une règle de filtrage d'URL qui comporte des spécifications de catégorie et de réputation. Toutes les demandes DNS qui correspondent à des règles antérieures dans la politique de contrôle d'accès à votre règle de filtrage d'URL contournent le filtrage de demande DNS. Ces requêtes DNS sont gérées selon la règle de correspondance, bloquées ou autorisées.

Inspection des intrusions, des fichiers et des logiciels malveillants

Les politiques de prévention des intrusions et de fichiers fonctionnent ensemble comme dernière ligne de défense avant que le trafic ne soit autorisé à atteindre sa destination :

- Les politiques de prévention des intrusions régissent les capacités de prévention des intrusions du système.
- Les politiques de fichiers régissent le contrôle des fichiers et les capacités de défense contre les programmes malveillants du système.

Tous les autres traitements de trafic ont lieu avant que le trafic réseau ne fasse l'objet d'un examen pour détecter les intrusions. En associant une politique de prévention des intrusions à une règle de contrôle d'accès, vous informez le système qu'avant que ne soit transmis le trafic correspondant aux conditions de la règle de contrôle d'accès, vous souhaitez inspecter le trafic au moyen d'une politique de prévention des intrusions.

Vous pouvez configurer des politiques de prévention des intrusions et des fichiers uniquement sur des règles qui **autorisent** le trafic. Aucune inspection n'est effectuée sur les règles définies pour attribuer la confiance (**trust**) à un trafic ou le bloquer (**block**). En outre, si l'action par défaut de la politique de contrôle d'accès est **allow**, vous pouvez configurer une politique de prévention des intrusions, mais pas une politique de fichiers.

Pour toute connexion unique gérée par une règle de contrôle d'accès, l'inspection des fichiers a lieu avant l'inspection de prévention des intrusions. C'est-à-dire que le système n'inspecte pas les fichiers bloqués par une politique de fichiers pour détecter les intrusions. Dans l'inspection des fichiers, le blocage simple par type prévaut sur l'inspection et le blocage des programmes malveillants. Jusqu'à ce qu'un fichier soit détecté et bloqué dans une session, les paquets de la session peuvent être soumis à une inspection de prévention des intrusions.



Remarque Par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès qui a configuré l'inspection des intrusions et des fichiers. L'inspection fonctionne uniquement avec le trafic non chiffré.

Bonnes pratiques pour l'ordre des règles de contrôle d'accès

Les règles sont appliquées sur la base de la première correspondance, vous devez donc vous assurer que les règles comprenant des critères de correspondance de trafic très spécifiques apparaissent au-dessus des politiques qui ont des critères plus généraux, qui s'appliqueraient autrement au trafic correspondant. Tenez compte des recommandations suivantes :

- Les règles spécifiques doivent précéder les règles générales, en particulier lorsqu'elles sont des exceptions aux règles générales.
- Toute règle qui rejette le trafic en se fondant uniquement sur des critères de couche 3/4 (comme l'adresse IP, la zone de sécurité et le numéro de port) devrait être placée le plus tôt possible. Nous vous recommandons de les placer avant toute règle nécessitant une inspection, comme celles avec des critères d'application ou d'URL, car les critères de la couche 3/4 peuvent être évalués rapidement et sans inspection. Bien entendu, toutes les exceptions à ces règles doivent être placées au-dessus.
- Chaque fois que cela est possible, mettez des règles de suppression spécifiques près du sommet de la politique. Cela garantit la prise de décision le plus tôt possible concernant le trafic indésirable.
- Les règles qui incluent à la fois des critères d'application et d'URL devraient être placées après les règles d'application uniquement ou d'URL uniquement, sauf si la règle application+URL constitue une exception à une règle plus générale d'application uniquement ou d'URL uniquement. Créez chaque fois que possible des règles distinctes pour le filtrage d'URL et d'application, car la combinaison des critères d'application et d'URL peut entraîner des résultats inattendus, en particulier pour le trafic chiffré.

NAT et critères d'accès

Les critères d'accès utilisent toujours les adresses IP réelles pour déterminer une correspondance, même si vous configurez la NAT. Par exemple, si vous configurez la NAT pour un serveur interne, 10.1.1.5, de sorte qu'il ait une adresse IP routable publiquement à l'extérieur, 209.165.201.5, alors le critère d'accès permettant au trafic externe d'accéder au serveur interne doit faire référence à l'adresse IP réelle du serveur (10.1.1.5), et non à l'adresse mappée (209.165.201.5).

Comment les autres politiques de sécurité impactent le contrôle d'accès

D'autres politiques de sécurité peuvent affecter le fonctionnement des règles de contrôle d'accès et la mise en correspondance des connexions. Lors de la configuration de vos critères d'accès, gardez les éléments suivants à l'esprit :

- **SSL Decryption policy** (Politique de déchiffrement SSL) : les règles de déchiffrement SSL sont évaluées avant le contrôle d'accès. Ainsi, si une connexion chiffrée correspond à une règle de déchiffrement SSL appliquant un type de déchiffrement, c'est la connexion en clair (déchiffrée) qui est évaluée par la stratégie de contrôle d'accès. Les règles de contrôle d'accès ne voient pas la version chiffrée de la connexion. De plus, toute connexion correspondant à une règle de déchiffrement SSL qui abandonne le trafic n'est jamais vue par la stratégie de contrôle d'accès. Enfin, toute connexion chiffrée correspondant à une règle Do Not Decrypt (Ne pas déchiffrer) est évaluée dans son état chiffré.
- **Identity policy** (Politique d'identité) : les connexions sont mises en correspondance avec les utilisateurs (et donc les groupes d'utilisateurs) uniquement s'il existe un mappage utilisateur pour l'adresse IP source. Les critères d'accès fondées sur l'appartenance à un utilisateur ou à un groupe ne peuvent correspondre qu'aux connexions pour lesquelles l'identité de l'utilisateur a été collectée avec succès par votre politique d'identité.
- **Security Intelligence policy** (Politique de renseignements de sécurité) : toute connexion abandonnée n'est jamais vue par la stratégie de contrôle d'accès. Les connexions correspondant à la liste Do Not Block (Ne pas bloquer) sont ensuite comparées aux règles de contrôle d'accès et, en définitive, c'est la règle de contrôle d'accès qui détermine le traitement de la connexion (autorisée ou abandonnée).
- **VPN** (site à site ou accès à distance) : le trafic VPN est toujours évalué par rapport à la stratégie de contrôle d'accès, et les connexions sont autorisées ou abandonnées selon la règle correspondante. Toutefois, le tunnel VPN lui-même est déchiffré avant l'évaluation de la stratégie de contrôle d'accès. La stratégie de contrôle d'accès évalue les connexions encapsulées dans le tunnel VPN, et non le tunnel lui-même.

Exigences de licence pour le contrôle d'accès

Vous n'avez pas besoin d'une licence spéciale pour utiliser la politique de contrôle d'accès.

Cependant, vous avez besoin des licences suivantes pour des fonctionnalités spécifiques dans la politique de contrôle d'accès. Pour en savoir plus sur la configuration des licences, consultez Activation ou désactivation des licences facultatives, à la page 95.

- Licence**URL** : pour créer des règles qui utilisent les catégories d'URL et les réputations comme critères de correspondance.
- Licence **Menace** : pour configurer une politique de prévention des intrusions sur une règle d'accès ou l'action par défaut. Vous avez également besoin de cette licence pour utiliser une politique de fichiers (la licence Programme malveillant est également requise).

- Licence **Programme malveillant** : pour configurer une politique de fichiers sur une règle d'accès. Le Menace est également requis pour les politiques de fichiers.

Lignes directrices et limites pour les stratégies de contrôle d'accès

Voici quelques limites supplémentaires pour le contrôle d'accès. Veuillez en tenir compte lors de l'évaluation si vous obtenez les résultats attendus de vos règles.

- Si une mise à jour de la base de données d'URL comprend des catégories ajoutées (nouvelles, entrantes), obsolètes (sortantes) ou supprimées, il existe un délai de grâce pour vous permettre d'apporter des modifications aux règles de contrôle d'accès concernées. Les règles concernées sont marquées de messages d'information, avec des descriptions des problèmes qui ont une incidence sur la règle et des liens vers le site web Cisco Talos Intelligence Group (Talos) pour obtenir plus d'informations sur les changements de catégorie. Vous devez mettre à jour la règle afin qu'elle utilise les catégories appropriées disponibles dans la dernière base de données d'URL.

  Pour tenir compte du délai de grâce, ajoutez les catégories entrantes nouvellement ajoutées aux règles appropriées sans supprimer les catégories obsolètes sortantes : vos règles doivent contenir les nouvelles et les anciennes catégories. Les nouvelles catégories entreront en vigueur lorsque les anciennes catégories seront marquées pour suppression. Lorsque les anciennes catégories sont finalement supprimées, vous devez modifier les règles pour supprimer les catégories supprimées et redéployer la configuration. Vous ne pourrez pas déployer la configuration jusqu'à ce que vous corrigiez les règles utilisant les catégories supprimées. Cliquez sur le lien **See Problem Rules** (Voir les règles problématiques) au-dessus du tableau pour filtrer les règles qui nécessitent votre attention.

- Gestionnaire de périphériques de pare-feu peut télécharger des informations sur un maximum de 50 000 utilisateurs à partir du serveur d'annuaire. Si votre serveur d'annuaire comprend plus de ce nombre de comptes utilisateur, vous ne verrez pas tous les noms possibles lors de la sélection des utilisateurs dans une règle d'accès ou lors de l'affichage des informations de tableau de bord basé sur l'utilisateur. Vous pouvez écrire des règles uniquement sur les noms qui ont été téléchargés.

  La limite s'applique également aux noms associés aux groupes. Si un groupe compte plus de la limite de membres, seuls les premiers noms téléchargés jusqu'à la limite peuvent être associés à l'appartenance au groupe.

- Si une mise à jour de la Vulnerability Database (VDB) retire (rend obsolètes) des applications, vous devez modifier toute règle de contrôle d'accès ou tout filtre d'application qui utilise l'application supprimée. Vous ne pouvez pas déployer les modifications avant d'avoir corrigé ces règles. En outre, vous ne pouvez pas installer les mises à jour du logiciel système avant de résoudre le problème. Dans la page d'objet des filtres d'application ou dans l'onglet Application de la règle, ces applications indiquent « (Deprecated) » (Obsolète) après le nom de l'application.

- Pour utiliser des objets réseau de nom de domaine complet (FQDN) comme critères de source ou de destination, vous devez également configurer DNS pour les interfaces de données dans **Device (Périphérique)** > **System Settings (Paramètres du système)** > **DNS Server (Serveur DNS)**. Le système n'utilise pas le paramètre du serveur DNS de gestion pour rechercher les objets de nom de domaine complet (FQDN) utilisés dans les règles de contrôle d'accès. Pour plus d'informations sur le dépannage de la résolution FQDN, consultez Dépannage des problèmes généraux de DNS, à la page 800.

Notez que le contrôle de l'accès par nom de domaine complet (FQDN) est un mécanisme du meilleur effort. Prenez en compte les points suivants:

- Étant donné que les réponses DNS peuvent être contrefaites, utilisez uniquement des serveurs DNS internes entièrement fiables.
- Certains noms de domaine complets, en particulier pour les serveurs très populaires, peuvent avoir des centaines, sinon des milliers d'adresses IP, et celles-ci peuvent changer fréquemment. Comme le système utilise les résultats de recherche DNS en cache, les utilisateurs peuvent obtenir des adresses qui ne sont pas encore dans le cache et leurs connexions ne correspondent pas à la règle FQDN. Les règles qui utilisent des objets réseau FQDN ne fonctionnent efficacement que pour les noms qui se résolvent en moins de 100 adresses.

  Nous vous recommandons de ne pas créer de règles d'objet réseau pour un nom de domaine complet qui se résout à plus de 100 adresses, car la probabilité que l'adresse d'une connexion en soit une qui a été résolue et disponible dans le cache DNS du périphérique est faible. Dans ces cas-là, utilisez une règle basée sur URL plutôt qu'une règle d'objet réseau FQDN.
- Pour les noms de domaine complets populaires, différents serveurs DNS peuvent renvoyer un ensemble d'adresses IP différent. Ainsi, si vos utilisateurs utilisent un serveur DNS différent de celui que vous configurez, les règles de contrôle d'accès basé sur le nom de domaine complet (FQDN) pourraient ne pas s'appliquer à toutes les adresses IP du site qui sont utilisées par vos clients, et vous n'obtiendrez pas les résultats escomptés pour vos règles .
- Certaines entrées de nom de domaine complet (FQDN) ont des valeurs de durée de vie très courte (TTL). Cela peut entraîner des recompilations fréquentes de la table de recherche, ce qui peut avoir une incidence sur les performances globales du système.

- Si vous modifiez une règle qui est activement utilisée, les modifications ne s'appliquent pas aux connexions établies qui ne sont plus inspectées par Snort. La nouvelle règle est utilisée pour la mise en correspondance avec les connexions futures. En outre, si Snort inspecte activement une connexion, il peut appliquer les critères de correspondance ou d'action modifiés à une connexion existante. Si vous devez vous assurer que vos modifications s'appliquent à toutes les connexions actuelles, vous pouvez vous connecter à l'interface de ligne de commande de l'appareil et utiliser la commande **clear conn** pour mettre fin aux connexions établies, en supposant que les sources tenteront ensuite de rétablir la connexion et seront ainsi correctement mises en correspondance avec la nouvelle règle.
- Il faut de 3 à 5 paquets pour que le système identifie l'application ou l'URL dans une connexion. Ainsi, la règle de contrôle d'accès correcte peut ne pas être mise en correspondance immédiatement pour une connexion donnée. Cependant, une fois que l'application ou l'URL est connue, la connexion est gérée en fonction de la règle de correspondance. Pour les connexions chiffrées, cela se produit après l'échange du certificat du serveur dans l'établissement de liaison SSL.
- Le système applique l'action de politique par défaut aux paquets qui n'ont pas de charge utile dans une connexion où une application est identifiée.
- Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Par exemple, le système peut faire correspondre plus efficacement le trafic pour toutes les interfaces si vous laissez simplement les critères de zone de sécurité vides, plutôt que si vous créez des zones qui contiennent toutes les interfaces. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.
- Si vous spécifiez des adresses IP pour les critères de source ou de destination, ne combinez pas les adresses IPv4 et IPv6 dans la même règle. Créez des règles distinctes pour les adresses IPv4 et IPv6.

- En raison de limites de mémoire, certains modèles de périphériques effectuent le filtrage d'URL avec une base de données plus petite de catégories et de réputations. Par exemple, même si les sous-sites d'une URL parente ont des catégories d'URL et une réputation différentes, certains périphériques peuvent ne stocker que les données de l'URL parente. Pour le trafic Web géré par ces périphériques, le système peut effectuer des recherches dans le nuage pour déterminer la catégorie et la réputation des sites qui ne figurent pas dans la base de données locale. Les périphériques à mémoire faible comprennent les modèles ASA suivants : 5508-X, 5516-X.
- Pendant son fonctionnement, le périphérique Firewall Threat Defense étend les règles de contrôle d'accès en plusieurs entrées de liste de contrôle d'accès en fonction du contenu de tout objet de réseau utilisé dans la règle d'accès. Vous pouvez réduire la mémoire requise pour rechercher des règles de contrôle d'accès en activant la recherche par groupe d'objets. Lorsque la recherche par groupe d'objets est activée, le système ne développe pas les objets réseau, mais recherche dans les critères d'accès les correspondances basées sur les définitions de ces groupes. La recherche par groupe d'objets n'a aucune incidence sur la façon dont vos critères d'accès sont définies ou sur la façon dont elles s'affichent dans FDM. Il a une incidence uniquement sur la façon dont le périphérique les interprète et les traite lors de la mise en correspondance des connexions avec les règles de contrôle d'accès.

  L'activation de la recherche de groupe d'objets réduit les besoins en mémoire pour les stratégies de contrôle d'accès qui incluent des objets réseau. Cependant, il est important de noter que la recherche par groupe d'objets peut également diminuer les performances de la recherche de règles et donc augmenter l'utilisation de l'unité centrale. Vous devez équilibrer l'incidence sur le processeur et le besoin en mémoire réduits pour la stratégie de contrôle d'accès spécifique. Dans la plupart des cas, l'activation de la recherche de groupe d'objets offre une nette amélioration opérationnelle.

  Vous pouvez définir cette option à l'aide de FlexConfig en envoyant la commande **object-group-search access-control** ; utilisez la forme **no** de la commande dans le modèle de négation.
- Les tunnels GRE qui enfreignent les RFC associées seront rejetés. Par exemple, si un tunnel GRE contient des valeurs non nulles dans les bits réservés, contrairement aux RFC, il est rejeté. Si vous devez autoriser les tunnels GRE non conformes, vous devez utiliser un gestionnaire distant et configurer une règle de préfiltre qui fait confiance aux sessions. Vous ne pouvez pas configurer de règles de préfiltre à l'aide de Gestionnaire de périphériques de pare-feu.

Configuration de la politique de contrôle d'accès

Utilisez la politique de contrôle d'accès pour contrôler l'accès aux ressources réseau. La politique consiste en un ensemble de règles ordonnées, qui sont évaluées de haut en bas. La règle appliquée au trafic est la première s'appliquant, entraînant la mise en correspondance de tous les critères de trafic. Si aucune règle ne correspond au trafic, l'action par défaut affichée au bas de la page est appliquée.

Pour configurer la politique de contrôle d'accès, sélectionnez **Policies** > **Access Control**.

Le tableau de contrôle d'accès répertorie toutes les règles dans l'ordre. Pour chaque règle :

- Cliquez sur le bouton > à côté du numéro de la règle dans la colonne la plus à gauche pour ouvrir le diagramme de règles. Le diagramme peut vous aider à visualiser comment la règle contrôle le trafic. Cliquez sur le bouton de nouveau pour fermer le diagramme.
- La plupart des cellules permettent la modification en ligne. Par exemple, vous pouvez cliquer sur l'action pour en sélectionner une autre, ou cliquer sur un objet réseau source pour ajouter ou modifier les critères source.

- Pour déplacer une règle, passez la souris sur la règle jusqu'à ce qu'apparaisse l'icône de déplacement (), puis sélectionnez la règle (en cliquant dessus), faites-la glisser et déposez-la au nouvel emplacement. Vous pouvez également déplacer une règle en la modifiant et en sélectionnant le nouvel emplacement dans la liste de l'ordre (**Order**). Il est essentiel que vous définissiez les règles dans l'ordre dans lequel vous souhaitez qu'elles soient traitée. Des règles spécifiques doivent être près du sommet, en particulier pour les règles qui définissent des exceptions s'appliquant aux règles plus générales.
- La colonne la plus à droite contient les boutons d'action pour une règle; passez la souris sur la cellule pour voir les boutons. Vous pouvez modifier () ou supprimer () une règle.
- Cliquez sur le bouton des **paramètres de contrôle d'accès** () pour configurer les paramètres qui s'appliquent à la politique de contrôle d'accès, plutôt qu'à des règles spécifiques dans la politique.
- Cliquez sur l'icône **Toggle Hit Counts** () au-dessus du tableau pour ajouter ou supprimer la colonne du nombre d'accès (Hit Counts) dans le tableau. Cette colonne apparaît à droite de la colonne du nom. Elle présente le nombre total d'accès à la règle et la date et l'heure du dernier accès. Les informations sur le nombre de visites sont extraites au moment où vous cliquez sur le bouton à bascule. Cliquez sur l'icône d'actualisation (**refresh**) () pour obtenir les dernières informations.
- Si des règles rencontrent des problèmes, par exemple en raison de catégories d'URL supprimées ou modifiées, cliquez sur le lien **See Problem Rules** (voir les règles pour lesquelles il y a des problèmes) à côté de la zone de recherche pour filtrer le tableau afin d'afficher uniquement ces règles. Veuillez modifier et corriger (ou supprimer) ces règles afin qu'elles fournissent le service dont vous avez besoin.

Les rubriques suivantes expliquent comment configurer la politique.

Configuration de l'action par défaut

Si une connexion ne correspond pas à une règle d'accès spécifique, elle est gérée par l'action par défaut de la politique de contrôle d'accès.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Étape 2 Cliquez n'importe où dans le champ **Default Action** (action par défaut).

Étape 3 Sélectionnez l'action à appliquer au trafic correspondant.

- **Trust** (confiance) : autorisez le trafic sans autre inspection d'aucune sorte.
- **Allow** (autoriser) : autorisez le trafic soumis à la politique d'intrusion.
- **Block** (blocage) : abandonne le trafic sans condition. Le trafic n'est pas inspecté.

Étape 4 Si l'action est **Allow** (autoriser), sélectionnez une politique de prévention des intrusions.

Pour obtenir une explication des options, consultez Paramètres de la politique de prévention des intrusions, à la page 526.

Étape 5 (Facultatif) Configurez la journalisation pour l'action par défaut.

Vous devez activer la journalisation du trafic correspondant à la règle pour qu'elle soit incluse dans les données du tableau de bord ou le visualisateur d'événements. Consultez Paramètres de journalisation, à la page 527

Étape 6 Cliquez sur **OK**.

Configuration des paramètres de la politique de contrôle d'accès

Vous pouvez configurer des paramètres qui s'appliquent à la politique de contrôle d'accès plutôt qu'à des règles spécifiques au sein de cette politique.

Procédure

Étape 1 Sélectionnez **Policy (Politique)** > **Access Control (Contrôle d'accès)**.

Étape 2 Cliquez sur le bouton **Access Policy Settings** (Paramètres de la politique d'accès) ( ).

Étape 3 Configurez les paramètres.

- **TLS Server Identity Discovery** (Découverte de l'identité du serveur TLS) : TLS 1.3 chiffre la plupart des messages d'établissement de liaison, de sorte que les renseignements sur les certificats ne sont pas facilement accessibles. Pour que le trafic chiffré avec TLS 1.3 corresponde aux règles d'accès qui utilisent le filtrage d'applications ou d'URL, le système doit disposer d'un certificat en clair pour le serveur. Si vous activez cette option, le système vérifie si un certificat pour le site est stocké en cache en fonction de l'adresse IP et de l'indication du nom du serveur (SNI) dans le paquet client « hello ». Si aucun certificat n'est disponible, le système utilise une sonde TLS 1.2 pour obtenir le certificat, qui pourra ensuite être utilisé pour identifier la catégorie et la réputation de l'application ou de l'URL. Nous vous recommandons d'activer cette option pour vous assurer que les connexions chiffrées correspondent à la bonne règle de contrôle d'accès. Ce paramètre sert uniquement à obtenir le certificat ; la connexion reste chiffrée. L'activation de cette option suffit pour obtenir les certificats TLS 1.3 ; vous n'avez pas besoin de créer une règle de déchiffrement SSL correspondante. Cependant, les certificats mis en cache sont aussi utilisés pour optimiser le traitement des règles de déchiffrement, en plus du traitement de contrôle d'accès.
- **Reputation Enforcement on DNS Traffic** (Application de la réputation sur le trafic DNS) : activez cette option pour appliquer vos règles de catégorie et de réputation de filtrage d'URL aux demandes de résolution DNS. Si le nom de domaine complet (FQDN) dans la demande de recherche dispose d'une catégorie et d'une réputation que vous bloquez, le système bloque la réponse DNS. Étant donné que l'utilisateur ne reçoit pas de résolution DNS, l'utilisateur ne peut pas établir la connexion. Utilisez cette option pour appliquer un filtrage de catégorie et de réputation d'URL au trafic non Web. Pour en savoir plus, consultez Filtrage des requêtes DNS, à la page 509.

Étape 4 Cliquez sur **OK**.

Configuration des règles de contrôle d'accès

Utilisez les règles de contrôle d'accès pour contrôler l'accès aux ressources réseau. Les règles de la stratégie de contrôle d'accès sont évaluées de haut en bas. La règle appliquée au trafic est la première s'appliquant, entraînant la mise en correspondance de tous les critères de trafic.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Étape 2 Effectuez l'une des actions suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle.

Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression ( ) de la règle.

Étape 3 Sous **Order**, sélectionnez l'endroit où vous souhaitez insérer la règle dans la liste ordonnée des règles.

Les règles sont appliquées sur la base de la première correspondance, vous devez donc vous assurer que les règles comprenant des critères de correspondance de trafic très spécifiques apparaissent au-dessus des politiques qui ont des critères plus généraux, qui s'appliqueraient autrement au trafic correspondant.

La valeur par défaut consiste à ajouter la règle à la fin de la liste. Si vous souhaitez modifier l'emplacement d'une règle ultérieurement, modifiez cette option.

Étape 4 Dans **Title** (titre), entrez un nom pour la règle.

Le nom ne peut pas contenir d'espaces. Vous pouvez utiliser des caractères alphanumériques et les caractères spéciaux suivants : + . _ -

Étape 5 Sélectionnez l'action à appliquer au trafic correspondant.

- **Trust** (confiance) : autorisez le trafic sans autre inspection d'aucune sorte.
- **Allow**(autorisation) : autorisez le trafic soumis à l'intrusion et à d'autres paramètres d'inspection dans la politique.
- **Block** (blocage) : abandonne le trafic sans condition. Le trafic n'est pas inspecté.

Étape 6 Définissez les critères de correspondance du trafic en utilisant n'importe quelle combinaison des onglets suivants :

- **Source/Destination** : zones de sécurité (interfaces) par lesquelles passe le trafic, adresses IP ou pays/continent (emplacement géographique) associé à l'adresse IP, balises de groupe de sécurité (SGT) attribuées à l'adresse, ou protocoles et ports utilisés par le trafic. La valeur par défaut englobe toute zone, adresse, emplacement géographique, SGT, protocole et port. Consultez Critères de source/de destination, à la page 519.
- **Application** : l'application ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. La valeur par défaut est n'importe quelle application. Consultez Critères d'application, à la page 521.
- **URL** : URL ou catégorie d'URL d'une demande Web ou d'une recherche DNS. La valeur par défaut est toute URL. Consultez Critères pour les URL, à la page 523.
- **Users** (Utilisateurs) : la source d'identité, l'utilisateur ou le groupe d'utilisateurs. Vos politiques d'identité déterminent si les informations d'utilisateur et de groupe sont disponibles pour la correspondance du trafic. Vous devez configurer les politiques d'identité pour utiliser ce critère. Consultez Critères utilisateur, à la page 524.

Pour modifier une condition, vous cliquez sur le bouton **+** dans cette condition, sélectionnez l'objet ou l'élément souhaité, puis cliquez sur **OK** dans la boîte de dialogue contextuelle. Si le critère requiert un objet, vous

pouvez cliquer sur **Create New *Object*** (créer un nouvel objet) si l'objet requis n'existe pas. Cliquez sur le **x** d'un objet ou d'un élément pour le supprimer de la politique.

Lorsque vous ajoutez des conditions aux règles de contrôle d'accès, tenez compte des conseils suivants :

- Vous pouvez configurer plusieurs conditions par règle. Le trafic doit correspondre à toutes les conditions de la règle pour que celle-ci s'applique au trafic. Par exemple, vous pouvez utiliser une règle unique pour effectuer le filtrage d'URL pour des hôtes ou des réseaux spécifiques.
- Pour chaque condition d'une règle, vous pouvez ajouter jusqu'à 50 critères. Le trafic qui correspond à l'un des critères d'une condition satisfait à la condition. Par exemple, vous pouvez utiliser une règle unique pour appliquer le contrôle d'application à 50 applications ou filtres d'application. Ainsi, il existe une relation OU entre les éléments d'une condition unique, mais une relation ET entre les types de condition (par exemple, entre la source ou destination et l'application).
- Certaines fonctionnalités nécessitent l'activation de la licence appropriée.

Étape 7 (Facultatif) Pour les politiques qui utilisent l'action Allow (Autoriser), vous pouvez configurer une inspection plus approfondie du trafic non chiffré. Cliquez sur l'un des liens suivants :

- **Intrusion Policy** (Politique de prévention des intrusions) : sélectionnez **Intrusion Policy (Politique de prévention des intrusions)** > **On (Activer)**, puis sélectionnez la politique d'inspection des intrusions afin d'inspecter le trafic à la recherche d'intrusions et d'exploits. Consultez Paramètres de la politique de prévention des intrusions, à la page 526.
- **File Policy** (Politique de fichiers) : sélectionnez la politique de fichiers afin d'inspecter le trafic pour détecter les fichiers contenant des programmes malveillants et les fichiers à bloquer. Consultez Paramètres de la stratégie de fichier, à la page 526.

Étape 8 (Facultatif) Configurez la journalisation pour la règle.

Par défaut, les événements de connexion ne sont pas générés pour le trafic qui correspond à une règle, bien que les événements de fichier soient générés par défaut si vous sélectionnez une politique de fichiers. Vous pouvez modifier ce comportement. Vous devez activer la journalisation du trafic correspondant à la politique pour qu'il apparaisse dans les données des tableaux de bord ou dans Event Viewer (Visionneuse d'événements). Consultez Paramètres de journalisation, à la page 527.

Des incidents d'intrusion sont toujours générés pour toute règle de prévention des intrusions définie pour bloquer ou alerter, quelle que soit la configuration de journalisation de la règle de contrôle d'accès correspondante.

Étape 9 Cliquez sur **OK**.

Critères de source/de destination

Les critères Source/Destination d'une règle d'accès définissent les zones de sécurité (interfaces) par lesquelles passe le trafic, les adresses IP ou le pays ou le continent (emplacement géographique) pour l'adresse IP, les balises du groupe de sécurité (SGT) assignées à l'adresse, ou les protocoles et les ports utilisés dans le trafic. La valeur par défaut englobe toute zone, adresse, emplacement géographique, SGT, protocole et port.

Pour modifier une condition, vous cliquez sur le bouton + dans cette condition, sélectionnez l'objet ou l'élément souhaité, puis cliquez sur **OK**. Si le critère requiert un objet, vous pouvez cliquer sur **Create New *Object*** (créer un nouvel objet) si l'objet requis n'existe pas. Cliquez sur le **x** d'un objet ou d'un élément pour le supprimer de la politique.

Vous pouvez utiliser les critères suivants pour identifier la source et la destination à mettre en correspondance dans la règle.

Zones source, zones de destination

Les objets de la zone de sécurité qui définissent les interfaces par lesquelles passe le trafic. Vous pouvez définir un critère, les deux critères ou aucun critère : tout critère non spécifié s'applique au trafic sur n'importe quelle interface.

- Pour faire correspondre le trafic sortant de l'appareil depuis une interface dans la zone, ajoutez cette zone aux **zones de destination**.
- Pour faire correspondre le trafic entrant dans l'appareil depuis une interface dans la zone, ajoutez cette zone aux zones source (**Source Zones**).
- Si vous ajoutez des conditions de zone source et de zone de destination à une règle, le trafic correspondant doit provenir de l'une des zones source spécifiées et sortir par l'une des zones de destination.

Utilisez ces critères lorsque la règle doit être appliquée en fonction de l'entrée ou de la sortie du trafic sur l'appareil. Par exemple, si vous voulez vous assurer que tout le trafic destiné aux hôtes internes est soumis à l'inspection d'intrusion, vous devez sélectionner votre zone interne comme **Destination Zones** (zones de destination) tout en laissant la zone source vide. Pour mettre en œuvre le filtrage des intrusions dans la règle, l'action liée à la règle doit être **Allow**(Autoriser), et vous devez sélectionner une politique de prévention des intrusions dans la règle.



Remarque Vous ne pouvez pas combiner des zones de sécurité passives et routées dans une seule règle. En outre, vous pouvez spécifier des zones de sécurité passives comme zones source uniquement, vous ne pouvez pas les spécifier comme zones de destination.

Réseaux sources, réseaux de destination

Les objets réseau ou les emplacements géographiques qui définissent les adresses réseau ou les emplacements du trafic.

- Pour faire correspondre le trafic d'une adresse IP ou d'un emplacement géographique, configurez les réseaux sources (**Source Networks**).
- Pour faire correspondre le trafic à une adresse IP ou à un emplacement géographique, configurez les réseaux de destination (**Source Networks**).
- Si vous ajoutez des conditions de réseau source et de destination à une règle, le trafic correspondant doit provenir de l'une des adresses IP spécifiées et être destiné à l'une des adresses IP de destination.

Lorsque vous ajoutez ce critère, vous sélectionnez les onglets suivants :

- **Network** (réseau) : Sélectionnez les objets ou groupes réseau qui définissent les adresses IP source ou de destination du trafic que vous souhaitez contrôler. Vous pouvez utiliser des objets qui définissent l'adresse utilisant le nom de domaine complet (FQDN); l'adresse est déterminée au moyen d'une recherche DNS.
- **Geolocation** (géolocalisation) : Sélectionnez l'emplacement géographique pour contrôler le trafic en fonction de son pays ou continent de source ou de destination. La sélection d'un continent sélectionne tous les pays du continent. En plus de sélectionner l'emplacement géographique

directement dans la règle, vous pouvez également sélectionner un objet de géolocalisation que vous avez créé pour définir l'emplacement. En utilisant la localisation géographique, vous pouvez facilement restreindre l'accès à un pays en particulier sans avoir besoin de connaître toutes les adresses IP potentielles qui y sont utilisées.



Remarque Pour vous assurer que vous utilisez des données de localisation géographique à jour pour filtrer votre trafic, Cisco vous recommande fortement de mettre à jour régulièrement la base de données de géolocalisation (GeoDB).

Ports source, ports/protocoles de destination

Les objets de port qui définissent les protocoles utilisés dans le trafic. Pour TCP/UDP, cela peut inclure les ports. Pour ICMP, cela peut inclure des codes et des type.

- Pour faire correspondre le trafic d'un protocole ou d'un port, configurez les ports source (**Source Ports**). Les ports source peuvent uniquement être TCP/UDP.
- Pour faire correspondre le trafic à un protocole ou à un port, configurez les protocoles/ports de destination (**Destination Ports/Protocols**). Si vous n'ajoutez que des ports de destination à une condition, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Les spécifications ICMP et les autres spécifications non TCP/UDP sont autorisées dans les ports de destination uniquement; elles ne sont pas autorisées pour les ports source.
- Pour faire correspondre le trafic provenant de ports TCP/UDP spécifiques et destiné à des ports TCP/UDP spécifiques, configurez les deux. Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP. Par exemple, vous pouvez cibler le trafic du port TCP/80 au port TCP/8080.

Groupes SGT source, groupes SGT de destination

Les objets de groupe de balise de groupe de sécurité (SGT) qui identifient les balises SGT affectées au trafic, tels qu'ils sont téléchargés à partir d'Identity Services Engine (ISE). Vous ne pouvez utiliser ces objets que si vous définissez une source d'identité Identity Services Engine (ISE) ; sinon, cette section ne s'affichera pas. Pour en savoir plus sur l'utilisation des balises SGT pour le contrôle d'accès, consultez Comment contrôler l'accès au réseau à l'aide des balises de groupe de sécurité TrustSec, à la page 532.

- Pour faire correspondre le trafic dont la source est l'une des balises SGT définies dans le groupe, configurez les **groupes SGT source**.
- Pour faire correspondre le trafic vers une destination dont l'une des balises SGT est définie dans le groupe, configurez les **groupes SGT de destination**.
- Si vous ajoutez des conditions de balise source et de destination à une règle, le trafic correspondant doit provenir d'une source avec l'une des balises spécifiées et être destiné à l'une des balises de destination.

Critères d'application

Les critères d'application d'une règle d'accès définissent l'application utilisée dans une connexion IP ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. La valeur par défaut est n'importe quelle application.

Bien que vous puissiez spécifier des applications individuelles dans la règle, les filtres d'applications simplifient la création et l'administration des politiques. Par exemple, vous pouvez créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible pertinence commerciale. Si un utilisateur tente d'utiliser l'une de ces applications, la session est bloquée.

De plus, Cisco met fréquemment à jour et ajoute des détecteurs d'applications supplémentaires par l'intermédiaire des mises à jour du système et de la base de données des vulnérabilités (VDB). Ainsi, une règle bloquant les applications à risque élevé peut s'appliquer automatiquement aux nouvelles applications sans que vous ayez à mettre à jour la règle manuellement.

Vous pouvez spécifier des applications et des filtres directement dans la règle, ou créer des objets de filtre d'application qui définissent ces caractéristiques. Les spécifications sont équivalentes, bien que l'utilisation d'objets puisse permettre de respecter plus facilement la limite du système de 50 éléments par critère si vous créez une règle complexe.

Pour modifier la liste des applications et des filtres, vous cliquez sur le bouton **+** dans la condition, sélectionnez les applications ou les objets de filtre d'application souhaités, qui sont répertoriés sur des onglets distincts, puis cliquez sur **OK** dans la boîte de dialogue contextuelle. Dans l'un ou l'autre des onglets, vous pouvez cliquer sur **Advanced Filter** (Filtres avancés) pour sélectionner des critères de filtre ou pour vous aider à rechercher des applications spécifiques. Cliquez sur le **x** pour une application, un filtre ou un objet pour le supprimer de la politique. Cliquez sur le lien **Save As Filter** (Enregistrer en tant que filtre) pour enregistrer les critères combinés qui ne sont pas déjà un objet en tant que nouvel objet de filtre d'application.



Remarque Si une application sélectionnée a été supprimée par une mise à jour de VDB, « (Deprecated) » s'affiche après le nom de l'application. Vous devez supprimer ces applications du filtre, sinon les déploiements et les mises à niveau logicielles du système suivants seront bloqués.

Vous pouvez utiliser les critères **Advanced Filter** (Filtres avancés) suivants pour identifier l'application ou le filtre à mettre en correspondance dans la règle. Il s'agit des mêmes éléments utilisés dans les objets de filtre d'application.



Remarque Plusieurs sélections dans un seul critère de filtre ont une relation OU. Par exemple, le risque est élevé ou très élevé. La relation entre les filtres est ET, donc le risque est élevé ou très élevé, ET la pertinence commerciale est faible ou très faible. Lorsque vous sélectionnez des filtres, la liste des applications dans l'affichage est mise à jour pour n'afficher que celles qui répondent aux critères. Vous pouvez utiliser ces filtres pour vous aider à trouver les applications que vous souhaitez ajouter individuellement ou pour vérifier que vous sélectionnez les filtres souhaités à ajouter à la règle.

Risques

La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation, de très faible à très élevée.

Pertinence commerciale

La probabilité que l'application soit utilisée dans le cadre des activités professionnelles de votre entreprise, plutôt qu'à des fins récréatives, de très faible à très élevée.

Types

Le type d'application :

- **Application Protocol** (Protocole d'application) : protocoles d'application tels que HTTP et SSH, qui représentent les communications entre les hôtes.
- **Client Protocol** (Protocole client) : clients tels que les navigateurs Web et les clients de messagerie, qui représentent les logiciels s'exécutant sur l'hôte.
- **Web Application** (Application Web) : applications Web telles que MPEG video et Facebook, qui représentent le contenu ou l'URL demandée pour le trafic HTTP.

Catégories

Une classification générale de l'application qui décrit sa fonction la plus essentielle.

Étiquettes

Des informations supplémentaires sur l'application, similaires à la catégorie.

Pour le trafic chiffré, le système peut identifier et filtrer le trafic en utilisant uniquement les applications marquées **SSL Protocol** (Protocole SSL). Les applications sans cette balise ne peuvent être détectées que dans le trafic non chiffré ou déchiffré. Le système attribue la balise de **trafic déchiffré** aux applications qu'il peut détecter dans le trafic déchiffré uniquement, non chiffré ou non déchiffré.

Liste des applications (bas de l'affichage)

Cette liste est mise à jour à mesure que vous sélectionnez des filtres dans les options au-dessus de la liste, de sorte que vous pouvez voir les applications qui correspondent actuellement au filtre. Utilisez cette liste pour vérifier que votre filtre cible les applications souhaitées lorsque vous avez l'intention d'ajouter des critères de filtre à la règle. Si votre intention est d'ajouter des applications spécifiques, sélectionnez-les dans cette liste.

Critères pour les URL

Les critères d'URL d'une règle d'accès définissent l'URL utilisée dans une demande Web ou la catégorie à laquelle l'URL demandée appartient. Pour les correspondances de catégorie, vous pouvez également spécifier la réputation relative des sites à autoriser ou à bloquer. La valeur par défaut est d'autoriser toutes les URL.

Si vous activez le filtrage de la demande de recherche DNS, les paramètres de catégorie et de réputation s'appliquent également au nom de domaine complet (FQDN) dans la demande de recherche. Seuls les paramètres de catégorie et de réputation s'appliquent au filtrage de demande DNS. Le filtrage manuel des URL est ignoré.

Les catégories d'URL et les réputations vous permettent de créer rapidement des conditions d'URL pour les règles de contrôle d'accès. Par exemple, vous pourriez bloquer tous les sites de jeu ou les sites de non fiables. Si un utilisateur tente de rechercher une URL avec cette catégorie et cette combinaison de réputation, la session est bloquée.

L'utilisation des données de catégorie et de réputation simplifie également la création et l'administration des politiques. Cela assure que le système contrôlera le trafic Web comme prévu. Enfin, comme les renseignements sur les menaces de Cisco sont continuellement mis à jour à la lumière de nouvelles URL, ainsi que de nouvelles catégories et risques pour les URL existantes, vous pouvez vous assurer que le système utilise des informations à jour pour filtrer les URL demandées. Les sites malveillants qui représentent des menaces de sécurité, comme les logiciels malveillants, les pourriels, les réseaux de zombies et l'hameçonnage peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer de nouvelles politiques.

Pour modifier la liste d'URL, cliquez sur le bouton + dans la condition, puis sélectionnez les catégories ou les URL souhaitées à l'aide de l'une des techniques suivantes. Cliquez sur le **x** pour une catégorie ou un objet afin de le supprimer de la politique.

Onglet URL

Cliquez sur le signe +, sélectionnez des objets ou des groupes d'URL, puis cliquez sur **OK**. Vous pouvez cliquer sur **Create New URL** (Créer une nouvelle URL) si l'objet dont vous avez besoin n'existe pas.



Remarque Avant de configurer des objets URL pour cibler des sites spécifiques, lisez attentivement les informations sur le filtrage d'URL manuel.

Onglet Catégories

Cliquez sur +, sélectionnez les catégories souhaitées, puis cliquez sur **OK**.

Pour une description des catégories, consultez https://www.talosintelligence.com/categories.

La valeur par défaut est d'appliquer la règle à toutes les URL de chaque catégorie sélectionnée, quelle que soit leur réputation. Pour limiter la règle en fonction de la réputation, cliquez sur la flèche vers le bas pour chaque catégorie, désélectionnez la case **Any** (Tout), puis utilisez le curseur **Reputation** (Réputation) pour choisir le niveau de réputation. À la gauche du curseur de réputation, vous trouverez de l'information sur les sites qui seront autorisés, tandis que les sites qui sont bloqués sont présentés du côté droit. La façon dont la réputation est utilisée dépend de l'action de la règle :

- Si la règle bloque ou surveille l'accès Web, la sélection d'un niveau de réputation sélectionne également toutes les réputations plus graves que ce niveau. Par exemple, si vous configurez une règle pour bloquer ou surveiller les sites (Suspects) et **Questionable** (Discutables) (niveau 2), elle bloque également automatiquement les sites (À risque élevé) et **Untrusted** (Non fiables) (niveau 1).
- Si la règle autorise l'accès Web, la sélection d'un niveau de réputation sélectionne également toutes les réputations moins graves que ce niveau. Par exemple, si vous configurez une règle pour autoriser les sites (Bénins) et **Favorable** (Favorables) (niveau 4), elle autorise également automatiquement les sites (Bien connus) et **Trusted (de confiance)** (niveau 5).

Sélectionnez l'option **Include Sites with Unknown Reputation** (inclure les sites avec une réputation inconnue) pour inclure les URL de réputation inconnue dans la correspondance de réputation. Les nouveaux sites ne sont généralement pas classés, et il peut y avoir d'autres raisons pour lesquelles la réputation d'un site est inconnue ou ne peut être déterminée.

Vérifier la catégorie d'une URL

Vous pouvez vérifier la catégorie et la réputation d'une URL particulière. Saisissez l'URL dans le champ **URL to Check** (URL à vérifier), puis cliquez sur **Go** (Lancer). Vous serez redirigé vers un site Web externe pour consulter les résultats. Si vous êtes en désaccord avec une catégorisation, cliquez sur le lien **Submit a URL Category** Dispute (Soumettre une contestation de catégorie d'URL) et faites-le-nous savoir.

Critères utilisateur

Les critères utilisateur d'une règle d'accès définissent l'utilisateur ou le groupe d'utilisateurs pour une connexion IP. Vous devez configurer les politiques d'identité et le serveur d'annuaire associé pour inclure les critères d'utilisateur ou de groupe d'utilisateurs dans une règle d'accès.

Vos politiques d'identité déterminent si l'identité de l'utilisateur est collectée pour une connexion particulière. Si l'identité est établie, l'adresse IP de l'hôte est associée à l'utilisateur identifié. Ainsi, le trafic dont l'adresse IP source est mappée à un utilisateur est considéré comme provenant de cet utilisateur. Les paquets IP en

eux-mêmes ne comprennent pas d'informations sur l'identité de l'utilisateur, de sorte que ce mappage adresse IP-utilisateur est la meilleure approximation disponible.

Étant donné que vous pouvez ajouter un maximum de 50 utilisateurs ou groupes à une règle, il est généralement plus logique de sélectionner des groupes que de sélectionner des utilisateurs individuels. Par exemple, vous pouvez créer une règle autorisant le groupe d'ingénierie à accéder à un réseau de développement, puis créer une règle ultérieure qui refuse tout autre accès au réseau. Ensuite, pour que la règle s'applique aux nouveaux ingénieurs, il vous suffit d'ajouter le spécialiste en ingénierie au groupe Engineering dans le serveur d'annuaire.

Vous pouvez également sélectionner les sources d'identité à appliquer à tous les utilisateurs de cette source. Ainsi, si vous prenez en charge plusieurs domaines Active Directory, vous pouvez fournir un accès différentiel aux ressources en fonction du domaine.

Pour modifier la liste des utilisateurs, vous cliquez sur le bouton **+** dans la condition et sélectionnez les identités souhaitées en utilisant l'une des techniques suivantes. Cliquez sur le **x** pour supprimer une identité de la politique.

- **Sources d'identité** : sélectionnez une source d'identité, telle qu'un domaine AD ou la base de données d'utilisateurs locaux, pour appliquer la règle à tous les utilisateurs obtenus à partir des sources sélectionnées. Si le domaine dont vous avez besoin n'existe pas encore, cliquez sur **Create New Identity Realm** (Créer un nouveau domaine d'identité) et créez-le maintenant.
- **Groupes** : sélectionnez les groupes d'utilisateurs souhaités. Les groupes sont disponibles uniquement si vous les configurez dans le serveur de répertoire. Si vous sélectionnez un groupe, la règle s'applique à tous les membres du groupe, y compris les sous-groupes. Si vous souhaitez traiter un sous-groupe différemment, vous devez créer une règle d'accès distincte pour le sous-groupe et la placer au-dessus de la règle pour le groupe parent dans la stratégie de contrôle d'accès.
- **Utilisateurs** : sélectionnez des utilisateurs individuels. Le nom d'utilisateur est précédé de la source d'identité, par exemple Realm\username (domaine\nom_utilisateur).

  Il existe certains utilisateurs intégrés dans le domaine Special-Identities-Realm (domaine d'identités spéciales) :

  - **Failed Authentication** (Échec de l'authentification) : l'utilisateur a été invité à s'authentifier, mais n'a pas réussi à saisir une paire nom d'utilisateur/mot de passe valide dans le nombre maximal de tentatives autorisées. L'échec de l'authentification n'empêche pas l'utilisateur d'accéder au réseau, mais vous pouvez écrire une règle d'accès pour limiter l'accès au réseau pour ces utilisateurs.
  - **Guest** (Invité) : les utilisateurs invités sont similaires aux utilisateurs en Failed Authentication (Échec de l'authentification), sauf que votre règle d'identité est configurée pour identifier ces utilisateurs comme Guest (Invité). Les utilisateurs invités ont été invités à s'authentifier et n'ont pas réussi à le faire dans les limites du nombre maximal de tentatives.
  - **No Authentication Required** (Aucune authentification requise) : l'utilisateur n'a pas été invité à s'authentifier, car ses connexions correspondaient à des règles d'identité ne spécifiant aucune authentification.
  - **Unknown** (Inconnu) : aucun mappage d'utilisateur n'existe pour l'adresse IP et aucun échec d'authentification n'a encore été enregistré. En règle générale, cela signifie qu'aucun trafic HTTP n'a encore été vu à partir de cette adresse.

Paramètres de la politique de prévention des intrusions

Cisco fournit plusieurs politiques d'intrusion avec le système de pare-feu. Les politiques d'intrusion fournies par Cisco Cisco Talos Intelligence Group (Talos) sont conçues par le Cisco.Talos, qui définit les états des règles d'intrusion et de préprocesseur ainsi que les paramètres avancés. Pour les règles de contrôle d'accès qui autorisent le trafic, vous pouvez sélectionner une politique d'intrusion pour inspecter le trafic à la recherche d'intrusions et d'exploits. Une politique de prévention des intrusions examine les paquets décodés à la recherche d'attaques basées sur des modèles, et peut bloquer ou modifier le trafic malveillant.

Lors de l'exécution de Snort 2, ce sont les seules politiques disponibles et vous ne pouvez pas les modifier. Cependant, vous pouvez modifier l'action à prendre pour une règle donnée, comme décrit dans Modification des actions des règles de prévention des intrusions (Snort 2), à la page 563.

Lors de l'exécution de Snort 3, vous pouvez sélectionner l'une de ces politiques ou créer vos propres politiques d'intrusion.

Pour activer l'inspection des intrusions, sélectionnez **Intrusion Policy (Politique d'intrusion)** > **On (Activée)** et sélectionnez la politique souhaitée. Cliquez sur l'icône d'information d'une politique dans la liste déroulante pour afficher une description pour chaque politique.

Pour en savoir plus sur les politiques prédéfinies, consultez Politiques d'analyse de réseau et de prévention des intrusions définies par le système, à la page 540.

Paramètres de la stratégie de fichier

Utilisez les politiques de fichiers pour détecter les programmes malveillants, ou *malware*, au moyen de la défense contre les logiciels malveillants. Vous pouvez également utiliser les politiques de fichiers pour effectuer le contrôle de fichier, ce qui permet de contrôler tous les fichiers d'un type spécifique, qu'ils contiennent ou non des logiciels malveillants.

La défense contre les logiciels malveillants utilise le Cisco AMP Cloud pour récupérer les dispositions relatives aux éventuels programmes malveillants détectés dans le trafic réseau, et pour obtenir des analyses locales de programmes malveillants et des mises à jour de pré-classification de fichiers. L'interface de gestion doit disposer d'un chemin vers Internet pour atteindre Cisco AMP Cloud et effectuer des recherches de programmes malveillants. Lorsque l'appareil détecte un fichier admissible, il utilise la valeur de hachage SHA-256 du fichier pour demander la Cisco AMP Cloud disposition du fichier. Les dispositions possibles sont les suivantes :

- Malware (Programmes malveillants) : le Cisco AMP Cloud a classé le fichier comme un logiciel malveillant. Un fichier d'archive (p. ex. un fichier compressé) est marqué comme malveillant si un de ses fichiers est malveillant.
- Clean (Propre : le Cisco AMP Cloud a classé le fichier comme propre, ne contenant aucun logiciel malveillant. Un fichier d'archive est marqué comme propre si tous les fichiers qu'il contient le sont.
- Unknown (Inconnu) : le Cisco AMP Cloud n'a pas encore affecté de disposition au fichier. Un fichier d'archive est marqué comme inconnu s'il contient un fichier inconnu.
- Unavailable (Non disponible) : le système n'a pas pu interroger le Cisco AMP Cloud pour déterminer la disposition du fichier. Vous pouvez voir un faible pourcentage d'événements avec cette disposition; c'est un comportement attendu. Si vous voyez un certain nombre d'événements « indisponible » se succéder, assurez-vous que la connexion Internet fonctionne correctement pour l'adresse de gestion.

Politiques de fichiers disponibles

Vous pouvez sélectionner l'une des politiques de fichiers suivantes :

- **Aucun** : n'évalue pas les fichiers transmis à la recherche de programmes malveillants et n'effectue aucun blocage spécifique aux fichiers. Sélectionnez cette option pour les règles dans lesquelles les transmissions de fichiers sont sécurisées ou lorsqu'elles sont peu probables (ou impossibles), ou pour les règles pour lesquelles vous êtes sûr que votre filtrage d'application ou d'URL protège adéquatement votre réseau.
- **Block Malware All** (Bloquer tous les programmes malveillants) : interrogez le Cisco AMP Cloudpour déterminer si des fichiers traversant votre réseau contiennent des programmes malveillants, puis bloquez les fichiers qui représentent des menaces.
- **Cloud Lookup All (Recherche dans le nuage pour tous)** : interrogez le Cisco AMP Cloud pour obtenir et consigner la disposition des fichiers traversant votre réseau, tout en autorisant leur transmission.
- **(Custom File Policy)** (Politique de fichiers personnalisée) : vous pouvez créer vos propres politiques de fichiers à l'aide de la ressource API filepolicies Firepower Threat Defense et des autres ressources FileAndMalwarePolicies (telles que filetypes, filetypecategories, ampcloudconfig, ampservers et ampcloudconnections). Après avoir créé les politiques et déployé les modifications, vous pouvez sélectionner vos politiques lors de la modification d'une règle de contrôle d'accès dans Gestionnaire de périphériques de pare-feu. La description de la politique s'affiche sous la politique lorsque vous la sélectionnez.

Paramètres de journalisation

Les paramètres de journalisation d'une règle d'accès déterminent si les événements de connexion sont émis pour le trafic qui correspond à la règle. Vous devez activer la journalisation pour voir les événements liés à la règle dans la visionneuse d'événements. Vous devez également activer la journalisation pour que le trafic correspondant soit reflété dans les différents tableaux de bord que vous pouvez utiliser pour surveiller le système.

Vous devez enregistrer les connexions en fonction des besoins de sécurité et de conformité de votre entreprise. Si votre objectif est de limiter le nombre d'événements que vous générez et d'améliorer les rendements, activez la journalisation uniquement pour les connexions essentielles à votre analyse. Toutefois, si vous souhaitez obtenir une vue d'ensemble de votre trafic réseau à des fins de profilage, vous pouvez activer la journalisation pour des connexions supplémentaires.



Mise en garde La journalisation des connexions TCP bloquées lors d'une attaque par déni de service (DoS) peut affecter le rendement du système et submerger la base de données avec plusieurs événements similaires. Avant d'activer la journalisation pour une règle de blocage, déterminez si la règle concerne une interface Internet ou une autre interface vulnérable aux attaques DoS.

Vous pouvez configurer les actions de journalisation suivantes.

Sélectionner l'action de journalisation

Vous pouvez sélectionner l'une des actions suivantes :

- **Log at Beginning and End of Connection** (Journaliser au début et à la fin de la connexion) : émet des événements au début et à la fin d'une connexion. Comme les événements de fin de connexion contiennent tout ce que contiennent les événements de début de connexion, ainsi que toutes les informations qui peuvent être obtenues au cours de la connexion, Cisco vous recommande de ne pas sélectionner cette option pour le trafic que vous autorisez. La journalisation de ces deux événements peut avoir une incidence sur les performances du système. Cependant, il s'agit de la seule option autorisée pour le trafic bloqué.

- **Log at End of Connection** (Journaliser à la fin de la connexion) : sélectionnez cette option si vous souhaitez activer la journalisation des connexions à la fin de la connexion, ce qui est recommandé pour le trafic autorisé ou de confiance.
- **No Logging at Connection** (Aucune journalisation à la connexion) : sélectionnez cette option pour désactiver la journalisation pour la règle. Il s'agit du paramètre par défaut.



Remarque Lorsqu'une politique de prévention des intrusions, invoquée par une règle de contrôle d'accès, détecte une intrusion et génère un événement d'intrusion, le système consigne automatiquement la fin de la connexion où l'intrusion s'est produite, quelle que soit la configuration de journalisation de la règle. Pour les connexions où une intrusion a été bloquée, l'action pour la connexion dans le journal de connexion est **Bloc**k (blocage), avec un motif **Intrusion Block** (blocage d'intrusion), même si, pour effectuer une inspection de prévention des intrusions, vous devez utiliser une règle Allow (autoriser).

Événements liés aux fichiers

Sélectionnez **Log Files** (Journaliser les fichiers) si vous souhaitez activer la journalisation des fichiers interdits ou des événements de programmes malveillants. Vous devez sélectionner une politique de fichiers dans la règle pour configurer cette option. L'option est activée par défaut si vous sélectionnez une politique de fichiers pour la règle. Cisco vous recommande de laisser cette option activée.

Lorsque le système détecte un fichier interdit, il consigne automatiquement l'un des types d'événement suivants :

- *File events* (événements de fichier), qui représentent les fichiers détectés ou bloqués, y compris les fichiers de programmes malveillants
- *Malware events* (événements de programmes malveillants), qui représentent uniquement les fichiers de programmes malveillants détectés ou bloqués
- *Retrospective malware events* (événements rétrospectifs de programme malveillant), qui sont générés lorsque la disposition de programme malveillant pour un fichier détecté précédemment change.

Pour les connexions où un fichier a été bloqué, l'action pour la connexion dans le journal de connexion est **Block** (blocage), même si, pour effectuer l'inspection des fichiers et des programmes malveillants, vous devez utiliser une règle Allow (autoriser). Le motif de la connexion (Reason) est soit **File Monitor** (surveillance de fichier, lorsqu'un type de fichier ou un programme malveillant a été détecté), soit **Malware Block** (blocage de programme malveillant) ou **File Block** (blocage de fichier), lorsqu'un fichier a été bloqué.

Envoyer les événements de connexion à :

Si vous souhaitez envoyer une copie des événements à un serveur syslog externe, sélectionnez l'objet serveur qui définit le serveur syslog. Si l'objet requis n'existe pas déjà, cliquez sur **Create New Syslog Server** (Créer un nouveau serveur syslog) et créez-le. (Pour désactiver la journalisation sur un serveur syslog, sélectionnez **Any** (N'importe lequel) dans la liste des serveurs.)

Comme le stockage d'événements sur l'appareil est limité, l'envoi des événements à un serveur journal système externe peut fournir un stockage à plus long terme et améliorer votre analyse des événements.

Ce paramètre s'applique uniquement aux événements de connexion. Pour envoyer les incidents d'intrusion à syslog, configurez le serveur dans les paramètres de la politique de prévention des intrusions. Pour envoyer des événements de fichier ou de programme malveillant à syslog, configurez le serveur dans

Device (Appareil) > **System Settings (Paramètres du système)** > **Logging Settings (Paramètres de journalisation)**.

Gestion des stratégies de contrôle d'accès

Les rubriques suivantes expliquent comment vous pouvez surveiller la stratégie de contrôle d'accès.

Statistiques de contrôle d'accès dans les tableaux de bord

La plupart des données sur les tableaux de bord **Monitoring** (Surveillance) sont directement liées à votre politique de contrôle d'accès. Consultez Tableaux de bord du trafic et du système, à la page 108.

- **Monitoring (Surveillance)** > **Access And SI Rules (Règles d'accès et SI)** affiche les règles d'accès les plus sollicitées, les équivalents de règles Security Intelligence et les statistiques associées.
- Vous pouvez trouver des statistiques générales dans les tableaux de bord **Network Overview** (Aperçu du réseau), **Destinations** et **Zones**.
- Vous pouvez trouver les résultats du filtrage d'URL dans les tableaux de bord (Catégories Web) **URL Categories** (Catégories d'URL) et **Destinations**. Vous devez avoir au moins une politique de filtrage d'URL pour voir des informations sur le tableau de bord **URL Categories (Catégories d'URL).**
- Vous pouvez trouver les résultats du filtrage des applications dans les tableaux de bord **Applications** et **Web Applications** (Applications Web).
- Vous pouvez trouver des statistiques basées sur les utilisateurs dans le tableau de bord **Users** (Utilisateurs). Vous devez mettre en œuvre des politiques d'identité pour recueillir les informations sur les utilisateurs.
- Vous pouvez trouver les statistiques relatives aux politiques de prévention des intrusions dans les tableaux de bord **Attackers** (Attaquants) et **Targets** (Cibles). Vous devez appliquer une politique de prévention des intrusions à au moins une règle de contrôle d'accès pour voir des informations dans ces tableaux de bord.
- Vous pouvez trouver les statistiques de politique de fichiers et de filtrage de programmes malveillants dans les tableaux de bord **File Logs** (Journaux de fichiers) et **Malware** (Programmes malveillants). Vous devez appliquer une politique de fichiers à au moins une règle de contrôle d'accès pour voir des informations dans ces tableaux de bord.
- **Monitoring (Surveillance)** > **Events (Événements)** affiche aussi les événements pour les connexions et les données liées aux règles de contrôle d'accès.

Examen du nombre de résultats pour les règles

Vous pouvez désormais afficher le nombre de résultats pour les règles de contrôle d'accès. Le nombre de résultats indique le nombre de connexions correspondant à la règle. Vous pouvez utiliser ces renseignements pour identifier les règles les plus actives et les règles qui sont moins actives.

Le nombre provient du dernier redémarrage du système, que ce soit à partir de votre action ou d'une mise à niveau du système, ou du moment où vous réinitialisez le nombre de résultats pour une règle ou toutes les règles.

Vous pouvez également afficher les informations sur le nombre de résultats dans les règles dans l'interface de ligne de commande du périphérique en utilisant la commande **show rule hits**.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Étape 2 Cliquez sur l'icône **Toggle Hit Counts** (Bascule du nombre de résultats) ( ).

Cette colonne apparaît à droite de la colonne du nom. Elle présente le nombre total d'accès à la règle et la date et l'heure du dernier accès. Les informations sur le nombre de visites sont extraites au moment où vous cliquez sur le bouton à bascule.

Vous pouvez effectuer les opérations suivantes avec les informations du nombre de résultats :

- À gauche du bouton, vous verrez des informations sur la dernière mise à jour du nombre de résultats.

  Cliquez sur l'icône **Refresh** (Actualiser) ( ) pour obtenir les derniers chiffres.

- Pour ouvrir une vue détaillée du nombre de résultats pour une règle donnée, cliquez sur le numéro de nombre de résultats dans le tableau pour ouvrir la boîte de dialogue Hit Count (Nombre de résultats). Les informations sur le nombre de résultats comprennent le nombre de résultats ainsi que la date et l'heure de la dernière connexion qui correspond à la règle. Cliquez sur le lien **Reset** (Réinitialiser pour réinitialiser le compteur à zéro.

  Si vous souhaitez réinitialiser le nombre de résultats pour toutes les règles en même temps, ouvrez une session SSH sur le périphérique et lancez la commande **clear rule hits**.

- Cliquez à nouveau sur l'icône **Toggle Hit Counts** (Bascule du nombre de résultats) ( ) pour supprimer la colonne du nombre d'accès (Hit Counts) du tableau.

Surveillance des messages Syslog pour le contrôle d'accès

En plus de voir les événements dans la visionneuse d'événements, vous pouvez configurer les règles de contrôle d'accès, les politiques de prévention des intrusions, les politiques de fichiers/programmes malveillants, et les politiques de Security Intelligence pour envoyer des événements à un serveur syslog. Les événements utilisent les ID de message suivants :

- 430001 : événement d'intrusion.
- 430002 : événement de connexion journalisé au début d'une connexion.
- 430003 : événement de connexion enregistré à la fin d'une connexion.
- 430004 : événements de fichier.
- 430005 : événements de programme malveillant.

Surveillance des stratégies de contrôle d'accès dans l'interface de ligne de commande

Vous pouvez également ouvrir la console d'interface de ligne de commande ou vous connecter à l'interface de ligne de commande du périphérique et utiliser les commandes suivantes pour obtenir des informations plus détaillées sur les stratégies de contrôle d'accès et les statistiques.

- **show access-control-config** affiche des informations récapitulatives sur les règles de contrôle d'accès ainsi que le nombre de résultats par règle.
- **show access-list** affiche les listes de contrôle d'accès (ACL) générées à partir des règles de contrôle d'accès. Les listes de contrôle d'accès fournissent un filtre initial et permettent de prendre rapidement des décisions lorsque c'est possible, afin que les connexions devant être abandonnées n'aient pas à être inspectées (et ne consomment donc pas de ressources inutilement). Ces renseignements comprennent le nombre de résultats.
- **show rule hits** affiche le nombre de résultats consolidés qui sont plus précis que les chiffres affichés avec **show access-control-config** et **show access-list**. Si vous souhaitez réinitialiser le nombre de résultats, utilisez la commande **clear rule hits**.
- **show snort statistics** affiche les renseignements sur le moteur d'inspection Snort, qui est l'inspecteur principal. Snort met en œuvre le filtrage des applications, le filtrage des URL, la protection contre les intrusions et le filtrage des fichiers et des programmes malveillants.
- **show conn** affiche les informations sur les connexions actuellement établies par les interfaces.
- **show traffic** affiche les statistiques sur le trafic circulant dans chaque interface.
- **show ipv6 traffic** affiche les statistiques sur le trafic IPv6 circulant dans le périphérique.

Exemples pour le contrôle d'accès

Le chapitre sur les cas d'utilisation comprend plusieurs exemples de mise en œuvre des règles de contrôle d'accès. Consultez les exemples suivants.

- Comment mieux comprendre le trafic de votre réseau, à la page 49. Cet exemple montre quelques concepts de base pour la collecte d'informations globales sur les connexions et les utilisateurs.
- Comment bloquer les menaces, à la page 56. Cet exemple montre comment appliquer les politiques de prévention des intrusions.
- Comment bloquer les logiciels malveillants, à la page 61. Cet exemple montre comment appliquer les politiques de fichiers.
- Comment mettre en œuvre une politique d'utilisation acceptable (filtrage d'URL), à la page 64. Cet exemple montre comment effectuer le filtrage d'URL.
- Comment contrôler l'utilisation des applications, à la page 69. Cet exemple montre comment effectuer le filtrage d'applications.
- Comment ajouter un sous-réseau, à la page 73. Cet exemple montre comment intégrer un nouveau sous-réseau à votre réseau global, y compris les règles d'accès nécessaires pour permettre la circulation du trafic.

• Comment surveiller passivement le trafic sur un réseau, à la page 78

Voici des exemples supplémentaires.

Comment contrôler l'accès au réseau à l'aide des balises de groupe de sécurité TrustSec

Si vous utilisez le moteur de services d'identité de Cisco (ISE) pour définir et utiliser la balise de groupe de sécurité (SGT) pour classer le trafic dans un réseau Cisco TrustSec, vous pouvez écrire des règles de contrôle d'accès qui utilisent la SGT comme critère de correspondance. Ainsi, vous pouvez bloquer ou autoriser l'accès en fonction de l'appartenance au groupe de sécurité plutôt que par rapport à des adresses IP.

À propos des balises de groupe de sécurité (SGT)

Dans Cisco Identity Services Engine (ISE), vous pouvez créer des balises de groupe de sécurité (SGT) et attribuer des adresses IP d'hôte ou de réseau à chaque balise. Vous pouvez également affecter des SGT aux comptes utilisateur, et la SGT est affectée au trafic de l'utilisateur. Si les commutateurs et les routeurs du réseau sont configurés pour le faire, ces balises sont ensuite affectées aux paquets à mesure qu'ils entrent dans le réseau contrôlé par ISE, le nuage Cisco TrustSec.

Lorsque vous configurez une source d'identité ISE dans le Gestionnaire de périphériques de pare-feu, le système Firepower Threat Defense télécharge automatiquement la liste des SGT à partir d'ISE. Vous pouvez ensuite utiliser SGT comme condition de correspondance de trafic dans les règles de contrôle d'accès.

Par exemple, vous pourriez créer une balise Utilisateurs de production et associer le réseau 192.168.7.0/24 à la balise. Ce serait approprié si vous utilisez ce réseau pour les points d'extrémité des utilisateurs, tels que les ordinateurs portables, les clients Wi-Fi et autres périphériques similaires. Vous pourriez créer une balise distincte pour les serveurs de production et attribuer les adresses IP des serveurs ou du sous-réseau concernés à la balise. Ensuite, dans le Firepower Threat Defense, vous pourriez autoriser ou bloquer l'accès du réseau d'utilisateurs aux serveurs de production en fonction de la balise. Si vous modifiez ultérieurement les adresses d'hôte ou de réseau associées à la balise dans ISE, vous n'avez pas besoin de modifier la règle de contrôle d'accès définie pour le périphérique Firepower Threat Defense.

Lorsqu'un périphérique Firepower Threat Defense évalue la balise SGT comme critère de correspondance de trafic pour une règle de contrôle d'accès, il utilise la priorité suivante :

1. La balise SGT source définie dans le paquet, le cas échéant. Pour que la balise SGT se trouve dans le paquet, les commutateurs et les routeurs du réseau doivent être configurés pour les ajouter. Consultez la documentation ISE pour obtenir des renseignements sur la mise en œuvre de cette méthode.
2. La balise SGT attribuée à la session utilisateur, telle que téléchargée à partir du répertoire de session ISE. Vous devez activer l'option d'écoute des informations de l'annuaire de session pour ce type de correspondance SGT, mais cette option est activée par défaut lorsque vous créez la source d'identité ISE pour la première fois. La balise SGT peut être mise en correspondance avec la source ou la destination. Bien que cela ne soit pas obligatoire, vous devez également configurer normalement une règle d'identité d'authentification passive, en utilisant la source d'identité ISE et un domaine AD, pour recueillir les informations sur l'identité de l'utilisateur.
3. Le mappage SGT-adresse IP téléchargé à l'aide de SXP. Si l'adresse IP se trouve dans la plage d'une SGT, le trafic correspond à la règle de contrôle d'accès qui utilise la SGT. La balise SGT peut être mise en correspondance avec la source ou la destination.

ISE utilise le protocole SXP (Security-group eXchange Protocol) pour propager la base de données de mappage IP-SGT vers les périphériques réseau. Lorsque vous configurez le périphérique Firepower Threat Defense pour utiliser un serveur ISE, vous devez activer l'option qui permet d'écouter le sujet SXP provenant d'ISE. Ainsi, le périphérique Firepower Threat Defense prend connaissance des balises et des mappages du groupe de sécurité directement auprès d'ISE et reçoit une notification chaque fois qu'ISE publie des balises et des mappages de groupe de sécurité mis à jour. Cela garantit que la liste des balises de groupe de sécurité et des mappages reste à jour sur le périphérique, afin que le périphérique Firepower Threat Defense puisse appliquer efficacement la politique définie dans ISE.

Configurer le contrôle d'accès en fonction de la balise de groupe de sécurité (SGT)

Pour configurer des règles de contrôle d'accès qui utilisent des balises de groupe de sécurité (SGT) comme critères de correspondance, vous devez d'abord configurer le périphérique pour obtenir les mappages SGT d'un serveur ISE.

La procédure suivante explique le processus de bout en bout basé sur l'hypothèse que vous souhaitez obtenir tous les mappages définis dans ISE, y compris les mappages SGT-adresses IP publiés par SXP. Vous pouvez aussi faire comme suit :

- Si vous souhaitez utiliser les informations SGT dans les paquets uniquement, et ne pas utiliser les mappages téléchargés à partir d'ISE, créez simplement des objets dynamiques de groupe SGT et utilisez-les comme critères SGT de source dans les règles de contrôle d'accès. Notez que dans ce cas, vous pouvez utiliser les balises SGT comme condition de source uniquement; ces balises ne correspondront jamais aux critères de destination.
- Si vous souhaitez utiliser SGT uniquement dans les paquets et les mappages SGT de session utilisateur, vous n'avez pas besoin d'activer l'option d'abonnement à la rubrique SXP dans la source d'identité ISE, ni de configurer ISE pour publier les mappages SXP. Vous pouvez utiliser ces informations pour les conditions de correspondance de source et de destination.

Avant de commencer

L'hypothèse ici est que vous avez déjà configuré Cisco TrustSec dans votre réseau et que vous ajoutez simplement l'appareil Firepower Threat Defense en tant que point d'application de la politique. Si vous n'avez pas déployé Cisco TrustSec, veuillez commencer par ISE et configurer votre réseau, puis revenez à cette procédure. L'explication de Cisco TrustSec n'entre pas dans le cadre de ce document.

Procédure

Étape 1 Assurez-vous que les balises SGT sont définies, qu'ISE est configuré correctement pour publier la rubrique SXP et que tous les mappages statiques nécessaires sont en place.

Consultez Configurer les groupes de sécurité et la publication SXP dans ISE, à la page 535.

Étape 2 Mettez à jour l'objet Identity Services Engine (Moteur de services d'identité) pour être à l'écoute de la rubrique SXP.

Vous pouvez utiliser ISE pour obtenir des mappages SGT de session utilisateur, des mappages SGT statiques d'adresses IP par l'intermédiaire de SXP, ou les deux. Par défaut, lorsque vous configurez la source d'identité ISE, elle obtient uniquement les mappages de session utilisateur; vous devez activer l'option d'écoute du sujet SXP d'ISE.

a) Choisissez **Objects (Objets)** > **Identity Sources (Sources d'identité)**.
b) Modifiez l'objet ISE. Si vous n'en avez pas encore configuré, cliquez sur **+** > **Identity Services Engine** (Moteur de services d'identité) et consultez Configurer Identity Services Engine (ISE), à la page 181.
c) Sous **Subscribe To** (S'abonner à), sélectionnez **SXP Topic** (Rubrique SXP).

   Assurez-vous que **Session Directory Topic** (Rubrique Session Directory) est également sélectionné si vous utilisez l'authentification passive ou si vous souhaitez des mappages utilisateur-SGT.



d) Cliquez sur **OK**.

Étape 3 Déployez vos modifications et attendez que le système télécharge les balises et les mappages à partir d'ISE.

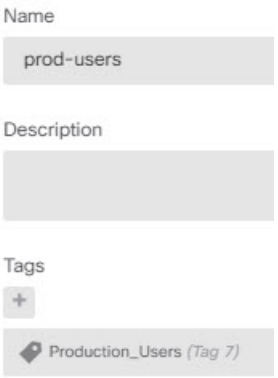
Après avoir configuré la source d'identité ISE et déployé les modifications, le système récupère les informations de balise de groupe de sécurité (SGT) à partir du serveur ISE. Le téléchargement ne se fera pas avant le déploiement des modifications.

Étape 4 Créez les objets de groupe SGT requis pour vos règles de contrôle d'accès.

Vous ne pouvez pas utiliser les informations extraites d'ISE directement dans une règle de contrôle d'accès. Au lieu de cela, vous devez créer des groupes SGT, qui font référence aux informations SGT téléchargées. Vos groupes de balises SGT peuvent faire référence à plusieurs SGT, vous pouvez donc appliquer une politique basée sur les collections de balises pertinentes, le cas échéant.

Le nombre et le contenu des objets dépendent des règles de contrôle d'accès que vous avez l'intention d'écrire. Répétez le processus suivant pour créer tous les objets dont vous avez besoin.

a) Choisissez **Objects (Objets)** > **SGT Groups (Groupes SGT)**.
b) Cliquez sur **+** pour ajouter un nouvel objet ou modifier un objet existant.
c) Pour les nouveaux objets, saisissez un nom et éventuellement une description.
d) Sous **Tags (Balises)**, cliquez sur **+** et sélectionnez toutes les balises à inclure dans le groupe.



e) Cliquez sur **OK**.

Étape 5 Créez des règles de contrôle d'accès qui utilisent les objets de groupe SGT.

Par exemple, la règle suivante autorise le trafic des utilisateurs de production vers les serveurs de production. La règle dépend entièrement des balises SGT ; elle n'est pas limitée par l'interface source/destination ni par tout autre critère. Ainsi, la règle s'appliquera dynamiquement au trafic, car il provient de différentes interfaces et à mesure que vous modifierez l'appartenance au groupe de sécurité dans ISE. Si le paquet ne contient pas

explicitement de SGT source, la correspondance de source/destination sera basée sur les adresses IP du paquet par rapport aux mappages SGT-adresses IP obtenus à partir des informations de session utilisateur ou des mappages publiés par SXP.

a) Choisissez **Politiques** > **Contrôle d'accès**.
b) Cliquez sur **+** pour créer une nouvelle règle ou modifier une règle existante.
c) Saisissez un nom de règle et sélectionnez **Allow** (Autoriser) comme action.
d) Dans l'onglet **Source/Destination**, cliquez sur **+** sous **Source** > **SGT Groups (Groupes SGT)**, puis sélectionnez l'objet que vous avez créé pour les utilisateurs de production.
e) Dans l'onglet **Source/Destination**, cliquez sur **+** sous **Destination** > **SGT Groups (Groupes SGT)** , et sélectionnez l'objet que vous avez créé pour les serveurs de production.
f) Configurez les autres options selon vos besoins. Par exemple, vous pouvez activer la journalisation et appliquer une politique de prévention des intrusions.
g) Cliquez sur **OK**.

Étape 6 Déployez la configuration.

Configurer les groupes de sécurité et la publication SXP dans ISE

Vous devez effectuer de nombreuses configurations dans Cisco Identity Services Engine (ISE) pour créer la politique TrustSec et les balises de groupes de sécurité (SGT). Veuillez consulter la documentation ISE pour des informations plus complètes sur la mise en œuvre de TrustSec.

La procédure suivante sélectionne les points saillants des paramètres principaux que vous devez configurer dans ISE pour que le périphérique Firepower Threat Defense puisse télécharger et appliquer les mappages statiques SGT-à-adresse IP, qui peuvent ensuite être utilisés pour la mise en correspondance SGT source et destination dans les règles de contrôle d'accès. Consultez la documentation d'ISE pour obtenir des informations détaillées.

Les captures d'écran de cette procédure sont basées sur ISE 2.4. Les chemins d'accès exacts à ces fonctionnalités pourraient changer dans les versions ultérieures, mais les concepts et les exigences seront les mêmes. Bien que la version 2.4 ou ultérieure d'ISE soit recommandée, de préférence la version 2.6 ou ultérieure, la configuration devrait fonctionner à partir du correctif 1 d'ISE 2.2.

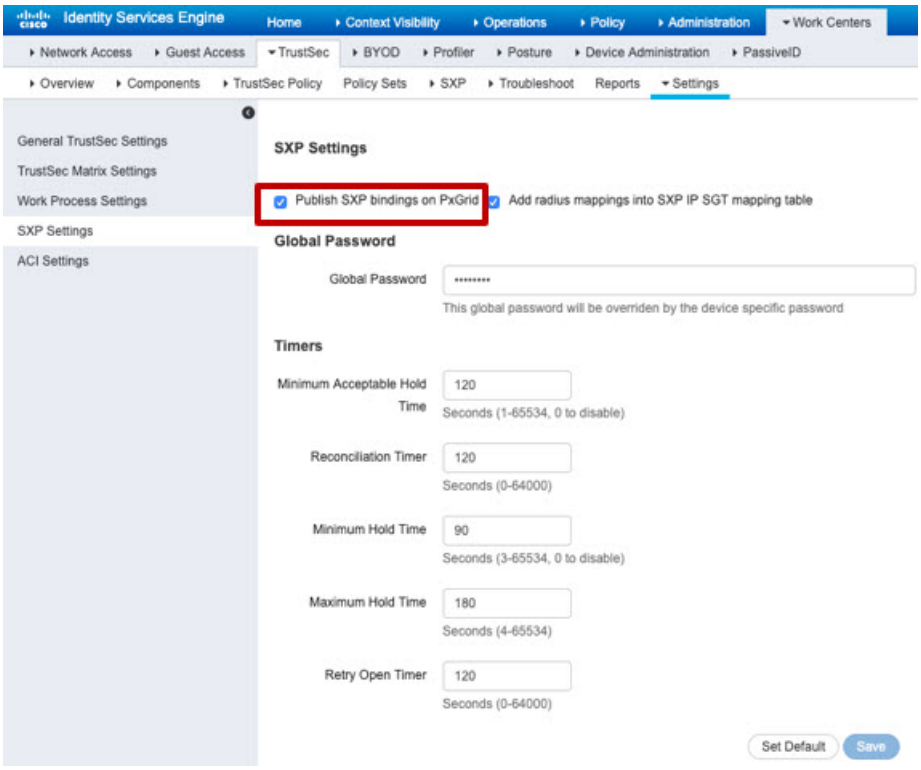
Avant de commencer

Vous devez posséder la licence ISE Plus pour publier les mappages statiques SGT-adresses IP et pour obtenir les mappages utilisateur session-SGT afin que le périphérique Firepower Threat Defense puisse les recevoir.

Procédure

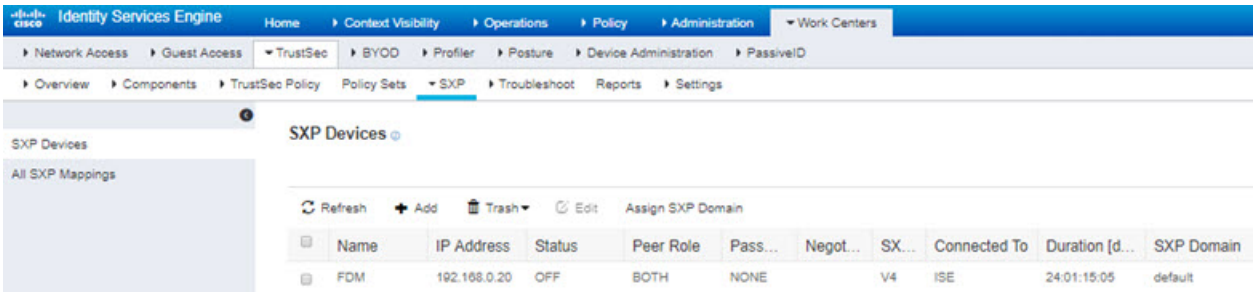
Étape 1 Choisissez **Work Centers** > **TrustSec** > **Settings** > **SXP Settings** > **(paramètres SXP)**, puis sélectionnez l'option **Publish SXP Bindings on PxGrid** (Publier les liens SXP sur PxGrid).

Cette option permet à ISE d'envoyer les mappages SGT à l'aide de SXP. Vous devez sélectionner cette option pour que le périphérique Firewall Threat Defense puisse « écouter » n'importe quel élément, de la liste au sujet SXP. Cette option doit être sélectionnée pour que le périphérique Firewall Threat Defense reçoive des informations de mappage SGT vers l'adresse IP statique. Ce n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets, ou les balises SGT qui sont attribuées à une session utilisateur.

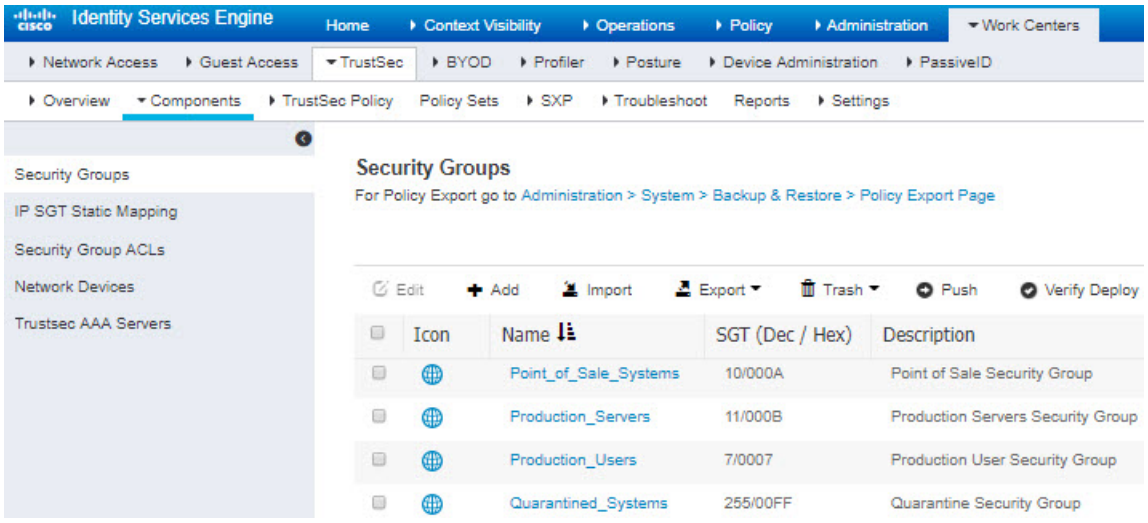


Étape 2 Choisissez **Work Centers** > **TrustSec** > **SXP** > **SXP Devices** (Centres de travail > TrustSec > SXP > Périphériques SXP) et ajoutez un périphérique.

Il n'est pas nécessaire que ce soit un périphérique réel, vous pouvez même utiliser l'adresse IP de gestion du périphérique Firepower Threat Defense. La table a simplement besoin d'au moins un périphérique pour amener ISE à publier les mappages statiques SGT- vers adresses IP. Cette étape n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets ou les balises SGT qui sont attribuées à une session utilisateur.

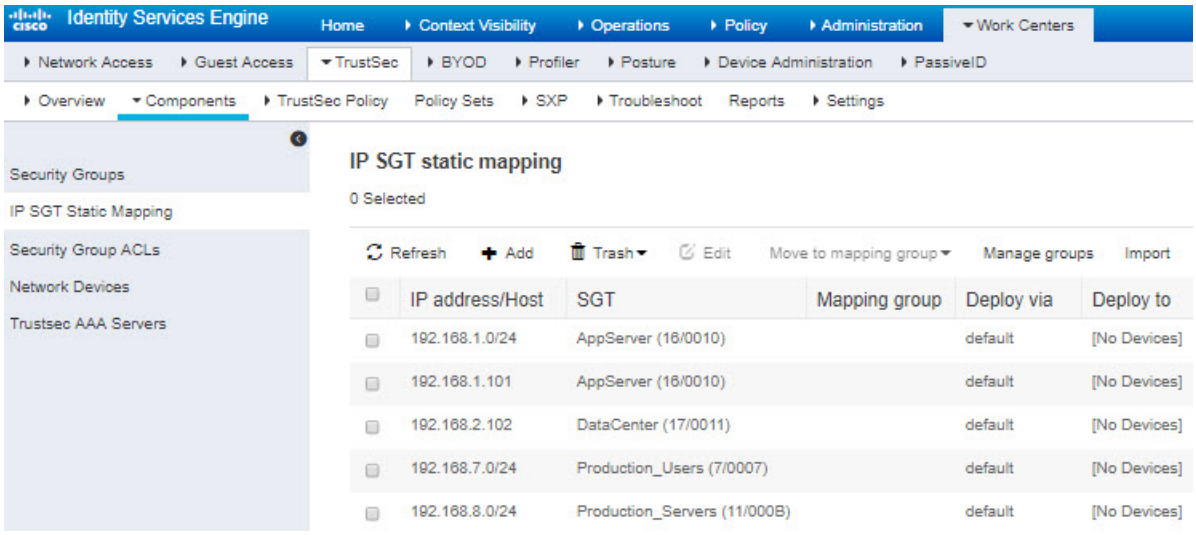


Étape 3 Choisissez **Work Centers** > **TrustSec** > **Components** > **Security Groups** (Centres de travail > TrustSec > Composants > Groupes de sécurité) et vérifiez que des balises de groupes de sécurité sont définies. Créez-en de nouveaux si nécessaire.



Étape 4 Choisissez **Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mapping** (Centres de travail > TrustSec > Composants > Mappage statique SGT IP) et mapper les adresses IP de l'hôte et du réseau aux balises du groupe de sécurité.

Cette étape n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets ou les balises SGT qui sont attribuées à une session utilisateur.





CHAPITRE 22

Stratégies de prévention des intrusions

Les rubriques suivantes expliquent les politiques de prévention des intrusions et les politiques d'analyse de réseau (Network Analysis Policy, NAP) associées. Les politiques de prévention des intrusions comprennent des règles qui vérifient le trafic pour détecter les menaces et bloquent le trafic qui semble être une attaque. Les politiques d'analyse de réseau contrôlent le prétraitement du trafic, qui prépare le trafic à une inspection plus approfondie en le normalisant et en relevant les anomalies de protocole.

Le prétraitement et l'inspection de prévention des intrusions sont si étroitement liés que les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet doivent se compléter mutuellement.

- À propos des politiques d'analyse de réseau et de prévention des intrusions, à la page 539
- Exigences de licence pour les politiques de prévention des intrusions, à la page 545
- Application des politiques de prévention des intrusions dans les règles de contrôle d'accès, à la page 545
- Commutation entre Snort 2 et Snort 3, à la page 546
- Configuration de Syslog pour les événements d'intrusion, à la page 547
- Gestion des politiques de prévention des intrusions Snort 3, à la page 548
- Gestion des politiques de prévention des intrusions (Snort 2), à la page 562
- Surveillance des politiques de prévention des intrusions, à la page 564
- Exemples de politiques de prévention des intrusions, à la page 564

À propos des politiques d'analyse de réseau et de prévention des intrusions

Les politiques d'analyse de réseau et de prévention des intrusions fonctionnent ensemble dans le cadre de la fonction de détection et de prévention des intrusions.

- Une politique d'analyse de réseau régit la façon dont le trafic est décodé et prétraité afin qu'il puisse être évalué de manière plus approfondie, en particulier pour détecter un trafic anormal qui pourrait signaler une tentative d'intrusion.
- Une politique de prévention des intrusions utilise des règles d'intrusion et de préprocesseur (parfois appelées collectivement règles de prévention des intrusions) pour examiner les paquets décodés à la recherche d'attaques basées sur des modèles. Les règles peuvent soit bloquer (abandon) le trafic menaçant et générer un événement, soit simplement le détecter (alerte) et générer uniquement un événement.

Pendant que le système analyse le trafic, la phase d'analyse de réseau (décodage et prétraitement) se produit avant et séparément de la phase de prévention des intrusions. Ensemble, les politiques d'analyse de réseau et

de prévention des intrusions permettent une inspection large et approfondie des paquets. Elles peuvent vous aider à détecter le trafic réseau, à vous alerter et à vous protéger contre le trafic réseau qui pourrait menacer la disponibilité, l'intégrité et la confidentialité des hôtes et de leurs données.

Politiques d'analyse de réseau et de prévention des intrusions définies par le système

Le système comprend plusieurs paires de politiques d'analyse de réseau et de prévention des intrusions du même nom, qui se complètent et fonctionnent ensemble. Par exemple, il existe des politiques de Politique d'analyse de réseau (NAP) et de prévention des intrusions nommées « Balanced Security and Connectivity », qui sont destinées à être utilisées ensemble. Les politiques fournies par le système sont configurées par Cisco Talos Intelligence Group (Talos). Pour ces politiques, Talos définit les états des règles de prévention des intrusions et de préprocesseur, et fournit les configurations initiales pour les préprocesseurs et d'autres paramètres avancés.

À mesure que de nouvelles vulnérabilités sont connues, Talos publie des mises à jour des règles de prévention des intrusions. Ces mises à jour de règles peuvent modifier toute analyse de réseau ou politique de prévention des intrusions fournie par le système, ainsi que des règles de prévention des intrusions et de préprocesseurs nouvelles ou mises à jour, des états modifiés pour les règles existantes et des paramètres de politique par défaut modifiés. Les mises à jour de règles peuvent également supprimer des règles des politiques fournies par le système et fournir de nouvelles catégories de règles, ainsi que modifier l'ensemble de variables par défaut.

Vous pouvez mettre à jour manuellement la base de données de règles ou configurer un calendrier de mise à jour réguliers. Vous devez redéployer une politique mise à jour pour que ses modifications prennent effet. Pour en savoir plus sur la mise à jour des bases de données du système, consultez Mise à jour des bases de données du système., à la page 821.

Voici les politiques fournies par le système :

Politiques d'analyse des intrusions et de sécurité et de connectivité équilibrées

Ces politiques sont conçues pour la vitesse et la détection. Utilisés ensemble, ils constituent un bon point de départ pour la plupart des organisations et des types de déploiement. Au départ, la politique d'analyse de réseau « Balanced Security and Connectivity » fournie par le système est la politique par défaut.

Politiques en matière d'analyse de réseau et de prévention des intrusions La connectivité avant la sécurité

Ces politiques sont conçues pour les organisations où la connectivité (permission d'accéder à toutes les ressources) prime sur la sécurité de l'infrastructure réseau. La politique de prévention des intrusions active beaucoup moins de règles que celles activées dans la politique de sécurité avant la connectivité. Seules les règles les plus critiques qui bloquent le trafic sont activées.

Politiques en matière d'analyse de réseau et de prévention des intrusions La connectivité avant la sécurité

Ces politiques sont conçues pour les réseaux où la sécurité de l'infrastructure réseau prime sur la facilité d'utilisation. La politique de prévention des intrusions permet d'appliquer de nombreuses règles de prévention des anomalies du réseau qui peuvent alerter sur le trafic légitime ou l'interrompre.

Politiques d'analyse de réseau et de prévention des intrusions

Ces politiques sont conçues pour les réseaux où la sécurité de l'infrastructure du réseau est encore plus importante que celle des politiques de sécurité sur la connectivité, avec un potentiel d'impact opérationnel encore plus grand. Par exemple, la politique de prévention des intrusions active des règles dans un grand nombre de catégories de menaces, y compris les programmes malveillants, les trousses d'exploit, les vulnérabilités anciennes et courantes, et les exploits connus et répandus.

Mode d'inspection : prévention ou détection

Par défaut, toutes les politiques de prévention des intrusions fonctionnent en mode de prévention pour mettre en œuvre un système de prévention des intrusions (IPS). En mode d'inspection de prévention, si une connexion correspond à une règle de prévention des intrusions dont l'action est d'abandonner le trafic, la connexion est activement bloquée.

Si vous souhaitez plutôt tester l'effet de la politique de prévention des intrusions sur votre réseau, vous pouvez passer au mode de détection, qui implémente un système de détection des intrusions (IDS). Dans ce mode d'inspection, les règles de rejet sont traitées comme des règles d'alerte, où vous êtes informé des connexions correspondantes, mais le résultat de l'action devient aurait bloqué, et les connexions ne sont jamais bloquées.

Vous modifiez le mode d'inspection par politique de prévention des intrusions, de sorte que vous pouvez avoir une combinaison de prévention et de détection.

Règles de prévention des intrusions et de préprocesseur

Une règle de prévention des intrusions est un ensemble précis de mots-clés et d'arguments que le système utilise pour détecter les tentatives d'exploitation des vulnérabilités de votre réseau. Lorsque le système analyse le trafic réseau, il compare les paquets aux conditions spécifiées dans chaque règle et déclenche la règle si le paquet de données répond à toutes les conditions spécifiées dans cette dernière.

Le système comprend les types de règles suivants, créés par Cisco Talos Intelligence Group (Talos) :

- lRègles de prévention des intrusions, subdivisées en règles d'objets partagés et en règles de texte standard
- Règles de préprocesseur, associées aux préprocesseurs et aux options de détection du décodeur de paquets dans la politique d'analyse de réseau. La plupart des règles de préprocesseur sont désactivées par défaut.

Les rubriques suivantes expliquent en détail les règles d'intrusion.

Attributs des règles d'intrusion

Lorsque vous affichez une politique de prévention des intrusions, vous voyez une liste de toutes les règles de prévention des intrusions disponibles pour identifier les menaces.

La liste de règles pour chaque politique est la même. La différence réside dans l'action configurée pour chaque règle. Comme il y a plus de 30 000 règles, le fait de faire défiler la liste prendra un certain temps. Les règles sont affichées à mesure que vous faites défiler la liste.

Voici les attributs qui définissent chaque règle :

> (Signature Description – Description de la signature)

Cliquez sur le bouton > dans la colonne de gauche pour ouvrir la description de la signature. La description est le code réel utilisé par le moteur d'inspection Snort pour faire correspondre le trafic à la règle. L'explication du code n'entre pas dans le cadre de ce document, mais il est expliquée en détail dans *le Guide de configuration du centre de gestion* ; sélectionnez le livre pour la version de votre logiciel dans http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html. Recherchez des informations sur la modification des règles de prévention des intrusions.

Les signatures contiennent des variables pour certains éléments. Pour en savoir plus, consultez Ensemble de variables d'intrusion par défaut, à la page 542.

GID

Identifiants de générateur (ID). Ce nombre indique quel composant du système évalue la règle et génère des événements. Un 1 indique une règle de prévention des intrusions de texte standard et un 3 indique une règle de prévention des intrusions d'objets partagés. (La différence entre ces types de règles n'est pas significative pour un utilisateur Gestionnaire de périphériques de pare-feu.) Il s'agit des principales règles d'intérêt lors de la configuration d'une politique de prévention des intrusions. Pour plus d'informations sur les autres GID, consultez Identifiants du Générateur, à la page 543.

SID

Identifiant (ID) Snort, également appelé ID de signature. Les ID Snort inférieurs à 1 000 000 ont été créés par Cisco Talos Intelligence Group (Talos).

Action

L'état de cette règle dans la politique de prévention des intrusions sélectionnée. Pour chaque règle, « (Default) » est ajouté à l'action qui est l'action par défaut pour la règle dans cette politique. Pour rétablir une règle à son paramètre par défaut, sélectionnez cette action. Les actions possibles sont :

- **Alert** (Alerte) : ce choix crée un événement lorsque cette règle correspond au trafic, sans interrompre la connexion.
- **Drop** (Abandon) : crée un événement lorsque cette règle correspond au trafic, puis interrompt la connexion.
- **Disabled** (Désactivé) : ne correspond pas au trafic avec cette règle. Aucun événement n'est généré.

État

Pour les règles Snort 2, l'état est une colonne distincte. Si vous modifiez l'action par défaut d'une règle, cette colonne affiche « Overridden » (Remplacé). Sinon, la colonne est vide.

Pour les règles Snort 3, l'état « Overridden » (Remplacé) s'affiche au bas de l'attribut Action, si vous l'avez modifié.

Message

Il s'agit du nom de la règle, qui apparaît également dans les événements déclenchés par la règle. Le message identifie généralement la menace à laquelle la signature correspond. Vous pouvez effectuer une recherche sur Internet pour obtenir plus d'informations sur chaque menace.

Ensemble de variables d'intrusion par défaut

Les signatures des règles de prévention des intrusions contiennent des variables pour certains éléments. Voici les valeurs par défaut pour les variables, $HOME_NET et $EXTERNAL_NET étant les variables les plus couramment utilisées. Notez que le protocole est spécifié séparément des numéros de port, donc les variables de port sont des numéros uniquement.

- $DNS_SERVERS = $HOME_NET (signifie toute adresse IP).
- $EXTERNAL_NET = toute adresse IP.
- $FILE_DATA_PORTS = $HTTP_PORTS, 143, 110.
- $FTP_PORTS = 21, 2100, 3535.
- $GTP_PORTS = 3386, 2123, 2152.
- $HOME_NET = toute adresse IP.

- $HTTP_PORTS = 144 ports numérotés : 36, 80-90, 311, 383, 443, 555, 591, 593, 631, 666, 801, 808, 818, 901, 972, 1158, 1212, 1220, 1414, 1422, 1533, 1741, 1830, 1942, 2231, 2301, 2381, 2578, 2809, 2980, 3029, 3037, 3057, 3128, 3443, 3507, 3702, 4000, 4343, 4848, 5000, 5117, 5222, 5250, 5450, 5600, 5814, 6080, 6173, 6767, 6988, 7000, 7001, 7005, 7071, 7080, 7144, 7145, 7510, 7770, 7777-7779, 8000, 8001, 8008, 8014, 8015, 8020, 8028, 8040, 8060, 8080-8082, 8085, 8088, 8118, 8123, 8161, 8180-8182, 8222, 8243, 8280, 8300, 8333, 8344, 8400, 8443, 8500, 8509, 8787, 8800, 8888, 8899, 8983, 9000, 9002, 9060, 9080, 9090, 9091, 9111, 9290, 9443, 9447, 9710, 9788, 9999, 10000, 11371, 12601, 13014, 15489, 19980, 23472, 29991, 33300, 34412, 34443, 34444, 40007, 41080, 44449, 50000, 50002, 51423, 53331, 55252, 55555, 56712.
- $HTTP_SERVERS = $HOME_NET (c'est-à-dire toute adresse IP).
- $ORACLE_PORTS = n'importe lequel
- $SHELLCODE_PORTS = 180.
- $SIP_PORTS = 5060, 5061, 5600
- $SIP_SERVERS = $HOME_NET (signifie toute adresse IP).
- $SMTP_SERVERS = $HOME_NET (signifie toute adresse IP).
- $SNMP_SERVERS = $HOME_NET (signifie toute adresse IP).
- $SQL_SERVERS = $HOME_NET (c'est-à-dire toute adresse IP).
- $SSH_PORTS = 22.
- $SSH_SERVERS = $HOME_NET (signifie n'importe quelle adresse IP).
- $TELNET_SERVERS = $HOME_NET (c'est-à-dire n'importe quelle adresse IP).

Identifiants du Générateur

L'identifiant de générateur (GID) identifie le sous-système qui évalue une règle de prévention des intrusions et génère des événements. Les règles de prévention des intrusions de texte standard ont un ID de générateur de 1, et les règles de prévention des intrusions d'objets partagés ont un ID de générateur de 3. Il existe également plusieurs ensembles de règles pour divers préprocesseurs. Le tableau suivant explique les GID.

Tableau 12 : ID de générateur

Identifiant	Composant
1	Règle de texte standard
2	Paquets balisés (Règles pour le générateur de balises, qui génère des paquets à partir d'une session balisée.)
3	Règle des objets partagés
102	Décodeur HTTP
105	Détecteur de Back Orifice
106	Décodeur de RPC

Identifiant	Composant
116	Décodeur de paquets
119, 120	Préprocesseur d’inspection HTTP (Les règles GID 120 se rapportent au trafic HTTP spécifique au serveur.)
122	Détecteur de balayage de ports
123	Défragmenteur d’adresses IP
124	Décodeur SMTP (Exploits contre les verbes SMTP.)
125	Décodeur FTP
126	Décodeur Telnet
128	Préprocesseur SSH
129	Préprocesseur de flux
131	Préprocesseur DNS
133	Préprocesseur DCE/RPC
134	Latence des règles, latence des paquets. (Les événements pour ces règles sont générés lorsque la latence des règles suspend (SID 1) ou réactive (SID 2) un groupe de règles d'intrusion, ou lorsque le système cesse d'inspecter un paquet parce que le seuil de latence des paquets est dépassé (SID 3).)
135	Détecteur d’attaque basé sur le débit (Connexions excessives aux hôtes du réseau.)
137	Préprocesseur SSL
138, 139	Préprocesseur de données sensibles
140	Préprocesseur SIP
141	Préprocesseur IMAP
142	Préprocesseur POP
143	Préprocesseur GTP
144	Préprocesseur Modbus
145	Préprocesseur DNP3

Stratégies d'analyse de réseau

Les politiques d'analyse de réseau contrôlent l'inspection prétraitement du trafic. Les préprocesseurs préparent le trafic à une inspection plus approfondie en le normalisant et en relevant les anomalies de protocole. Le prétraitement lié à l'analyse de réseau a lieu après la mise en correspondance des renseignements de sécurité et le déchiffrement SSL, mais avant le début de l'intrusion ou de l'inspection des fichiers.

Par défaut, le système utilise la politique d'analyse de réseau Sécurité et connectivité équilibrées pour prétraiter tout le trafic géré par une stratégie de contrôle d'accès. Toutefois, si vous configurez une politique de prévention des intrusions sur n'importe quelle règle de contrôle d'accès, le système utilise la politique d'analyse de réseau qui correspond à la politique de prévention des intrusions la plus agressive appliquée. Par exemple, si vous utilisez à la fois des politiques de sécurité sur la connectivité et des politiques équilibrées dans vos règles de contrôle d'accès, le système utilise la Politique d'analyse de réseau (NAP) de sécurité sur la connectivité pour tout le trafic. Pour les politiques de prévention des intrusions personnalisées Snort 3, cette affectation est effectuée conformément à la politique de modèle de base attribuée à la politique de prévention des intrusions.

Exigences de licence pour les politiques de prévention des intrusions

Vous devez disposer de la licence **Menace** pour appliquer des politiques d'intrusion dans les règles d'accès. Pour en savoir plus sur la configuration des licences, consultez Activation ou désactivation des licences facultatives, à la page 95.

Aucune licence supplémentaire n'est nécessaire pour les politiques d'analyse de réseau.

Application des politiques de prévention des intrusions dans les règles de contrôle d'accès

Pour appliquer les politiques de prévention des intrusions au trafic réseau, vous sélectionnez la politique dans une règle de contrôle d'accès qui autorise le trafic. Vous n'attribuez pas directement de politiques de prévention des intrusions.

Vous pouvez attribuer différentes politiques de prévention des intrusions pour fournir une protection contre les intrusions variable en fonction des risques relatifs des réseaux que vous protégez. Par exemple, vous pourriez utiliser la politique de sécurité sur la connectivité, plus stricte, pour le trafic entre votre réseau interne et les réseaux externes. D'un autre côté, vous pouvez appliquer la politique de connectivité sur la sécurité, plus clémente, pour le trafic entre les réseaux internes.

Vous pouvez également simplifier votre configuration en utilisant la même politique pour tous les réseaux. Par exemple, la politique de sécurité et de connectivité équilibrée est conçue pour fournir une bonne protection sans affecter excessivement la connectivité.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Étape 2 Créez une nouvelle règle ou modifiez une règle existante qui **autorise** le trafic.

En outre, vous pouvez configurer une politique de prévention des intrusions dans le cadre de l'action par défaut si l'action par défaut est allow (autoriser).

Vous ne pouvez pas appliquer de politiques de prévention des intrusions aux règles qui font confiance ou bloquent le trafic.

Étape 3 Cliquez sur l'onglet **Intrusion Policy** (politique de prévention des intrusions).

Étape 4 Sélectionnez **Intrusion Policy** > **On** (Politique d'intrusion activée) et sélectionnez la politique d'inspection des intrusions à utiliser pour le trafic correspondant.

Commutation entre Snort 2 et Snort 3

Snort est le moteur d'inspection principal du produit. Bien que vous puissiez changer de version de Snort librement, certaines règles de prévention des intrusions dans Snort 2.0 peuvent ne pas exister dans Snort 3.0, et inversement. Si vous avez modifié l'action d'une règle existante, cette modification n'est pas conservée si vous passez à Snort 3, puis de nouveau à Snort 2, ou de nouveau à Snort 3. Vos modifications apportées aux actions de règles pour les règles qui existent dans les deux versions sont conservées. Notez que le mappage entre les règles dans Snort 3 et Snort 2 peut être un à un ou un à plusieurs, de sorte que la conservation des modifications se fait au mieux.

Si vous modifiez la version de Snort, le système effectuera un déploiement automatique pour mettre en œuvre la modification. Vous pouvez voir la progression dans la Task list (liste des tâches). Les tâches sont Snort Version Change (changement de version Snort) et Automatic Deployment—Snort version toggle (déploiement automatique — basculement de version Snort). En raison du déploiement et du fait que Snort doit être arrêté et redémarré, toutes les connexions existantes, y compris le VPN, sont abandonnées et doivent être rétablies, ce qui entraînera une perte momentanée du trafic.



Remarque Si vous essayez de permuter les versions Snort et que le commutateur échoue, vous aurez des modifications en attente que vous ne pouvez pas ignorer, et une tentative de basculement ultérieure ne sera pas autorisée. Si cela se produit, vous devez effectuer le basculement à l'aide de l'API ToggleInspectionEngine, que vous pouvez utiliser à partir de l'explorateur d'API. Vous devez définir l'attribut bypassPendingChangeValidation à TRUE.

Avant de commencer

Pour déterminer quelle version de Snort est actuellement activée, utilisez cette procédure ou choisissez **Policies (Politiques)** > **Intrusion**. Recherchez la ligne **Snort Version** (Version Snort) au-dessus du tableau. La version actuelle est le premier numéro du numéro de version complet. Par exemple, 2.9.17-95 est une version Snort 2.

Si le périphérique se trouve dans un réseau isolé, considérez le téléversement manuel du dernier ensemble de règles pour la nouvelle version avant le basculement.

Si vous passez à la version 2.0, toutes les politiques de prévention des intrusions personnalisées que vous avez créées sont converties dans les politiques de base utilisées dans la politique personnalisée. Dans la mesure du possible, les remplacements d'actions de règles sont conservés. Si plusieurs politiques personnalisées utilisent la même politique de base, les remplacements de la politique personnalisée utilisée dans la plupart des politiques de contrôle d'accès sont conservés et les remplacements des autres politiques personnalisées sont perdus. Les règles de contrôle d'accès qui utilisaient ces politiques « en double » utiliseront désormais la politique de base

créée à partir de votre politique personnalisée la plus utilisée. Toutes les politiques personnalisées sont supprimées. Si vous souhaitez conserver les politiques personnalisées afin de pouvoir les importer ultérieurement, après être passé à Snort 3, utilisez l'API Firewall Threat Defense pour exporter la configuration.

Vous devez déployer toutes les modifications en attente avant de pouvoir changer de version Snort.

Procédure

Étape 1 Sélectionnez **Device** (Périphérique), puis cliquez sur **View Configuration** (Afficher la configuration) dans le résumé des Updates (mises à jour).

Regardez le groupe **Intrusion Rule** (Règles de prévention des intrusions. La version actuelle de Snort est indiquée.

Étape 2 Dans le groupe **Intrusion Rule** (Règles de prévention des intrusions, vous pouvez modifier la version de Snort en cliquant sur **Upgrade to Snort 3.0** (Mise à niveau vers Snort 3.0) ou **Downgrade to Snort 2.0** (Rétrograder à Snort 2.0).

Étape 3 Lorsque vous y êtes invité, sélectionnez l'option d'obtention du dernier ensemble de règles de prévention des intrusions, puis cliquez sur **Yes** (Oui).

Nous vous recommandons d'obtenir le dernier paquet de règles. Le système télécharge les paquets pour la version Snort active uniquement. Il est donc peu probable que le dernier paquet soit installé pour la version Snort vers laquelle vous passez.

Vous devez attendre la fin de la tâche de commutation de versions avant de pouvoir modifier les politiques de prévention des intrusions.

Configuration de Syslog pour les événements d'intrusion

Vous pouvez configurer un serveur syslog externe afin que les politiques de prévention des intrusions envoient des événements d'intrusion à votre serveur syslog. Vous devez configurer le serveur syslog dans la politique de prévention des intrusions pour que les événements d'intrusion soient envoyés au serveur. La configuration d'un serveur syslog sur une règle d'accès envoie uniquement les événements de connexion au serveur syslog, et non les événements d'intrusion.

Si vous sélectionnez plusieurs serveurs syslog, les événements sont envoyés à chacun d'eux.

Les incidents d'intrusion ont l'ID de message 430001.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **Intrusion (Prévention des intrusions)**.

Étape 2 Cliquez sur le bouton **Edit Logging Settings (Modifier les paramètres de journalisation)** (⚙) pour configurer syslog.

Étape 3 Cliquez sur le bouton + sous **Send Intrusion Events To (envoyer les événements d'intrusion à)** et sélectionnez les objets de serveur qui définissent les serveurs syslog. Si les objets requis n'existent pas déjà, cliquez sur **Create New Syslog Server** (Créer un serveur syslog) et créez-les.

Étape 4 Cliquez sur **OK**.

Gestion des politiques de prévention des intrusions Snort 3

Lorsque vous utilisez Snort 3 comme moteur d'inspection, vous pouvez créer vos propres politiques de prévention des intrusions et les personnaliser en fonction de vos besoins. Le système est livré avec des politiques prédéfinies qui sont basées sur des politiques définies portant le même nom Cisco Talos Intelligence Group (Talos). Bien que vous puissiez modifier ces politiques, il est préférable de créer votre propre politique à partir de la politique Talos sous-jacente et de modifier celle-ci si vous devez ajuster les actions des règles.

Chacune de ces politiques prédéfinies comprend la même liste de règles de prévention des intrusions (également appelées signatures), mais elles diffèrent par les actions appliquées pour chaque règle. Par exemple, une règle peut être activée dans une politique, mais désactivée dans une autre.

Si vous trouvez qu'une règle particulière vous donne trop de faux positifs, où la règle bloque le trafic que vous ne souhaitez pas bloquer, vous pouvez désactiver la règle sans avoir à passer à une politique de prévention des intrusions moins sécurisée. Vous pouvez également le modifier pour qu'il soit signalé par une alerte pour les correspondances sans perte du trafic.

Inversement, si vous savez que vous devez vous protéger contre une attaque spécifique, mais que la règle associée est désactivée dans la politique de prévention des intrusions de votre choix, vous pouvez activer la règle sans passer pour une politique plus sécurisée.

Utilisez les tableaux de bord liés aux intrusions et le Visualiseur d'événement (tous deux sur la page **Monitoring** (Surveillance)) pour évaluer l'incidence des règles de prévention des intrusions sur le trafic. Gardez à l'esprit que vous ne verrez les incidents d'intrusion et les données de prévention des intrusions que pour le trafic qui correspond aux règles de prévention des intrusions définies sur « alerte » ou « abandon »; les règles désactivées ne sont pas évaluées.

Remarque Si vous passez à Snort 2, vous ne pouvez pas créer de politiques personnalisées, et l'utilisation des politiques de prévention des intrusions diffère légèrement. Au lieu de cette rubrique, consultez Gestion des politiques de prévention des intrusions (Snort 2), à la page 562.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Vérifiez que la version de Snort affichée au-dessus du tableau est 3.x.

Étape 2 Effectuez l'une des actions suivantes :

- Utilisez la zone **Search/Filter** (Recherche/filtre) pour trouver une politique. Vous pouvez effectuer une recherche par nom uniquement.

- Cliquez sur l'icône en forme d'engrenage ( ) pour activer la journalisation sur un serveur syslog. Consultez Configuration de Syslog pour les événements d'intrusion, à la page 547.
- Cliquez sur + pour créer une nouvelle politique. Consultez Configuration d'une politique de prévention des intrusions personnalisée (Snort 3), à la page 549.
- Cliquez sur l'icône de modification ( ) pour voir les propriétés et les règles de la politique et pour les modifier. Consultez Affichage ou modification des propriétés de la politique de prévention des intrusions (Snort 3), à la page 550.
- Cliquez sur l'icône de suppression ( ) pour supprimer une politique.

Configuration d'une politique de prévention des intrusions personnalisée (Snort 3)

Vous pouvez créer de nouvelles politiques de prévention des intrusions pour personnaliser le comportement des règles si les politiques prédéfinies ne répondent pas à vos besoins. En général, il est conseillé de créer des politiques personnalisées en fonction des politiques prédéfinies plutôt que de modifier ces politiques. Cela vous garantit de pouvoir facilement mettre en œuvre l'une des politiques définies par Cisco Talos si vous trouvez que vos personnalisations ne fournissent pas les résultats dont vous avez besoin.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle politique, cliquez sur +.
- Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle. Lorsque les détails de la politique sont affichés, cliquez sur le lien **Edit** (Modifier) dans la section des propriétés de la politique en haut de la page.

Étape 3 Saisissez un **nom** et, éventuellement, une description pour cette politique.

Étape 4 Configurez le **mode d'inspection** pour la politique.

- **Prevention** (Prévention) : les actions découlant d'une règle d'intrusion sont toujours appliquées. Les connexions correspondant à une règle de suppression sont bloquées.
- **Détection** : les règles d'intrusion génèrent uniquement des alertes. Une connexion qui correspond à une règle de suppression génère des messages d'alerte, mais la connexion n'est pas bloquée.

Étape 5 Sélectionnez le **modèle de base** pour la politique.

Les modèles de base sont fournis par Cisco Talos. Cliquez sur l'icône d'information pour chacun pour voir plus d'informations sur les politiques. Notez que les noms de politiques peuvent changer et que de nouvelles politiques peuvent apparaître lorsqu'un nouveau paquet de règles est installé.

- **Détection maximale (Cisco Talos)** : cette politique met l'accent sur la sécurité. La connectivité et le débit du réseau ne sont pas garantis, et des faux positifs sont probables. Cette politique ne doit être utilisée que pour les zones à sécurité élevée, et les moniteurs de sécurité doivent être prêts à enquêter sur les alertes pour déterminer leur validité.
- **Sécurité avant connectivité (Cisco Talos)** : cette politique met l'accent sur la sécurité, au détriment éventuel de la connectivité et du débit du réseau. Le trafic est inspecté plus en profondeur, davantage de règles sont évaluées, et l'on peut s'attendre à des faux positifs et à une augmentation de la latence, mais dans des limites raisonnables.
- **Sécurité et connectivité équilibrées (Cisco Talos)** : (Par défaut.) Cette politique tente de trouver un équilibre subtil entre la connectivité et le débit du réseau, d'une part, et les besoins en matière de sécurité, d'autre part. Bien qu'elle ne soit pas aussi stricte que la politique Sécurité avant connectivité, cette politique vise à assurer la sécurité des utilisateurs tout en étant moins gênante pour le trafic normal.
- **Connectivité avant sécurité (Cisco Talos)** : cette politique met l'accent sur la connectivité et le débit du réseau, au détriment éventuel de la sécurité. Le trafic est inspecté plus superficiellement et moins de règles sont évaluées.
- **Aucune règle active (Cisco Talos)** : il s'agit d'une politique de base qui configure les paramètres de préprocesseur typiques, mais qui n'a aucune règle ni alerte intégrée activée. Utilisez cette politique comme base si vous souhaitez vous assurer que seules les politiques que vous souhaitez appliquer sont activées.

Étape 6 Cliquez sur **OK**.

Vous êtes renvoyé à la liste des politiques de prévention des intrusions. Vous pouvez maintenant afficher la nouvelle politique et ajuster les actions des règles au besoin.

Affichage ou modification des propriétés de la politique de prévention des intrusions (Snort 3)

La page Intrusion Policy (politique de prévention des intrusions) affiche une liste des politiques, y compris les politiques prédéfinies et définies par l'utilisateur, et leurs descriptions. Pour modifier une politique, vous devez d'abord afficher les propriétés de la politique.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

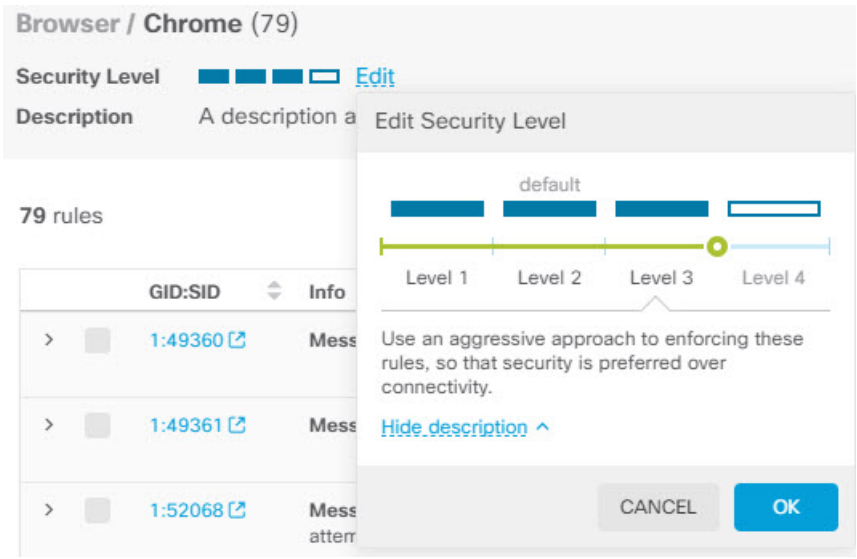
Étape 2 Cliquez sur l'icône de modification ( ) d'une politique.

La politique comprend les sections suivantes :

- Liste déroulante **Policy Name (Nom de la politique)**.
  - Vous pouvez facilement passer à une autre politique en la sélectionnant dans la liste déroulante ou revenir à la liste des politiques en cliquant sur le bouton de retour ( ).

- Vous pouvez supprimer cette politique en cliquant sur l'icône de suppression à côté du nom de la politique ( ).

- **Propriétés générales**. Cette section affiche le mode de prévention des intrusions, la politique de base et la description. Cliquez sur **Edit (Modifier)** pour modifier ces propriétés ou le nom de la politique.
- Table des matières **Rule Group** (Groupe de règles). Cette liste affiche tous les groupes de règles qui ont des règles actives dans la politique. Les groupes ont une hiérarchie, avec des groupes parents contenant des groupes enfants qui organisent des sous-ensembles de règles dans le groupe parent plus grand. Chaque groupe est un ensemble logique de règles, et une règle donnée peut apparaître dans plusieurs groupes.
  - Pour ajouter un groupe qui ne comporte actuellement aucune règle active dans la politique, cliquez sur + > **Add Existing Rule Group** (Ajouter un groupe de règles existant) et sélectionnez le groupe. Consultez Ajout ou suppression de groupes de règles dans une politique de prévention des intrusions (Snort 3), à la page 553.
  - Pour modifier le niveau de sécurité d'un groupe, sélectionnez le groupe enfant dans la liste. La liste des règles change pour afficher le niveau de sécurité en haut, avec les règles du groupe répertoriées ci-dessous. Cliquez sur le lien **Edit** (Modifier) à côté du niveau de sécurité et sélectionnez un nouveau niveau. Cliquez sur **View Description** (Afficher la description) lors de la modification pour obtenir des renseignements sur chaque niveau de sécurité. Notez que la modification du niveau peut changer les règles actives, ainsi que l'action pour une règle donnée, les niveaux plus sécurisés ayant tendance à avoir davantage de règles actives et plus de règles avec l'action Drop (Abandon). Cliquez sur **OK** pour confirmer la modification. (Le niveau de sécurité ne s'applique pas aux groupes de règles personnalisées.)



- Pour supprimer toutes les règles d'un groupe, sélectionnez le groupe enfant dans la liste. Ensuite, cliquez sur le lien **Exclude** (Exclure) à l'extrémité droite du nom du groupe et confirmez que vous souhaitez exclure le groupe. L'exclusion du groupe désactive simplement toutes les règles du groupe. Cela ne supprime pas le groupe.

  Toutefois, si le groupe comprend des règles partagées avec d'autres groupes activés, les règles partagées conservent toutes les actions appliquées par le groupe toujours actif. Dans tous les cas, nous conservons votre paramètre le plus strict pour une règle individuelle, quelle que soit l'appartenance au groupe.

- Pour ajouter un nouveau groupe de règles personnalisées, cliquez sur **+** > **Upload Custom Rules** (Charger des règles personnalisées) . Pour de plus amples renseignements, consultez la section Chargement de règles de prévention des intrusions personnalisées, à la page 558.
- Pour modifier le nom ou la description d'un groupe de règles personnalisées, cliquez sur **Edit** (Modifier).
- Pour supprimer un groupe de règles personnalisées, cliquez sur **Delete** (Supprimer). Pour en savoir plus, consultez Gestion des règles de prévention des intrusions personnalisées et des groupes de règles, à la page 556.
- Pour ajouter une nouvelle règle personnalisée dans un groupe de règles personnalisées, cliquez sur le signe **+** au-dessus du tableau de règles. Consultez Configuration des règles de prévention des intrusions personnalisées individuelles, à la page 560.
- Pour modifier, dupliquer, supprimer ou gérer l'appartenance à un groupe pour une règle personnalisée, passez le curseur sur la droite de la règle et cliquez sur le bouton ou la commande approprié. Pour en savoir plus, consultez Configuration des règles de prévention des intrusions personnalisées individuelles, à la page 560.

- **List of rules** (Liste des règles). Vous pouvez utiliser le champ de recherche pour vous aider à trouver des règles à l'aide de la recherche en texte intégral. Vous pouvez également sélectionner des éléments de filtrage pour effectuer une recherche sur n'importe quelle combinaison de GID ou SID, afficher uniquement les règles définies par l'utilisateur (celles que vous avez ajoutées), ou simplement afficher les règles en fonction de leurs actions : Disabled (désactivée), Alert (alerte) ou Drop (Abandon). Les règles sont chargées au fur et à mesure, de sorte qu'il faut un certain temps pour faire défiler l'ensemble de la liste non filtrée. Lors du filtrage de la liste, cliquez sur le bouton Refresh (Actualiser) pour recharger l'affichage filtré.
  - Pour modifier l'action pour une règle, cliquez sur la case **Action** pour la règle et sélectionnez la nouvelle action, **Alert only** (Alerter uniquement), **Block matching traffic** (Bloquer le trafic correspondant) ou **Disable** (Désactiver). L'action par défaut pour chaque règle est indiquée.
  - Pour modifier l'action pour plus d'une règle à la fois, cochez la case dans la colonne de gauche des règles que vous souhaitez modifier, puis sélectionnez la nouvelle action dans la liste déroulante **Action** au-dessus du tableau des règles. Cochez la case dans l'en-tête GID:SID pour sélectionner toutes les règles de la liste. Vous pouvez modifier jusqu'à 5 000 règles à la fois.
  - Pour mettre à jour les règles dans un groupe de règles personnalisé, cliquez sur **Upload Rule File** (Charger le fichier de règles). Pour en savoir plus, consultez Chargement de règles de prévention des intrusions personnalisées, à la page 558.
  - Pour obtenir plus d'informations sur une règle, cliquez sur le lien dans la case **GID:SID**. Le lien vous mène vers Snort.org.
  - Pour modifier les règles répertoriées, vous pouvez cliquer sur un groupe enfant dans la table des matières du groupe de règles (et non sur un groupe parent). Vous pouvez revenir à la liste de toutes les règles en cliquant sur **ALL RULES** (TOUTES les règles) en haut de la liste des groupes de règles.

- Pour modifier l'ordre de tri, cliquez sur l'en-tête de tableau d'une colonne. Le tri par défaut des règles affiche d'abord les règles remplacées, puis celles dont l'action est Drop (abandon), puis celles dont l'action est Alert (alerte).

Ajout ou suppression de groupes de règles dans une politique de prévention des intrusions (Snort 3)

Les règles de prévention des intrusions sont structurées en groupes locaux. Il existe une hiérarchie entre les groupes, avec des groupes parents contenant des groupes enfants associés. Les règles elles-mêmes ne s'affichent que dans les groupes enfants : les groupes parents sont simplement une structure organisationnelle. Une règle donnée peut apparaître dans plusieurs groupes.

Tous les groupes de règles personnalisées que vous créez se trouvent dans le dossier Groupes définis par l'utilisateur. Les groupes de règles personnalisées n'ont pas de hiérarchie.

La façon la plus simple d'ajouter ou de supprimer des règles dans une politique de prévention des intrusions est d'ajouter ou de supprimer des groupes. Comme les règles d'un groupe sont logiquement liées, il est fort possible que vous souhaitiez utiliser la plupart, si ce n'est toutes les règles d'un groupe donné.

La procédure suivante explique comment ajouter des groupes et modifier le niveau de sécurité du groupe.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur l'icône Edit (Modifier) ( ) pour le compte que vous souhaitez modifier.

Étape 3 (Ajout de groupes.) Si le groupe ne s'affiche pas dans la liste des groupes de règles, cliquez sur **+** > **Add Existing Rule Group** (Ajouter un groupe de règles existant) et procédez comme suit :

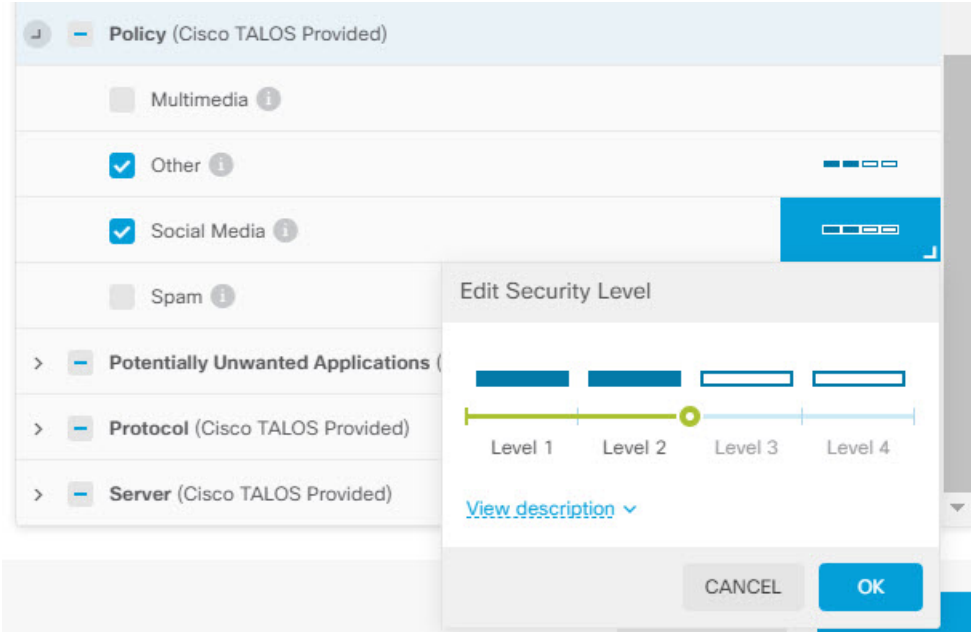
a) Recherchez le groupe enfant.

- Une coche à côté du nom d'un groupe parent indique que tous les groupes enfants du groupe parent sont déjà sélectionnés.
- Un signe moins à côté d'un nom de groupe parent indique qu'un ou plusieurs groupes enfants ne présentent aucune règle activée pour cette politique. Ce sont les groupes que vous pouvez ajouter.
- Une coche à côté d'un nom de groupe enfant indique que le groupe est déjà sélectionné.

b) Sélectionnez le groupe que vous souhaitez ajouter (c'est-à-dire cochez sa case).

c) (Facultatif, ne s'applique pas aux groupes de règles personnalisées.) Chaque groupe a un niveau de sécurité par défaut dépendant de la politique de base utilisée pour la politique personnalisée. Si vous souhaitez le modifier, cliquez sur l'icône du niveau de sécurité, sélectionnez un nouveau niveau, puis cliquez sur **OK**.

Le niveau 1 est la posture la moins sécurisée, car il met l'accent sur la connectivité plutôt que sur la sécurité, tandis que le niveau 4 est la posture la plus stricte et offre une sécurité maximale. Vous pouvez cliquer sur **View Description (Afficher la description)** pour voir une explication de chaque niveau lorsque vous le sélectionnez.



d) Continuez à sélectionner (ou à désélectionner) des groupes jusqu'à ce que vous ayez apporté toutes vos modifications.

e) Cliquez sur **OK**.

Étape 4 (Suppression de groupes.) Si vous souhaitez désactiver toutes les règles dans un groupe, vous pouvez utiliser l'une des méthodes suivantes :

- Sélectionnez le groupe, puis cliquez sur le lien **Exclude** (Exclure) à l'extrémité droite du nom du groupe, au-dessus de la liste des règles.
- Utilisez la méthode pour ajouter un groupe, mais désélectionnez le groupe indésirable (c'est-à-dire décochez sa case) et cliquez sur **OK**.
- Vous pouvez supprimer un groupe de règles personnalisées pour le retirer entièrement du système et de toutes les politiques de prévention des intrusions qui l'utilisent. Sélectionnez le groupe, puis cliquez sur **Delete** (Supprimer).

Modification des actions des règles de prévention des intrusions (Snort 3)

Chaque politique de prévention des intrusions a les mêmes règles. La différence est que l'action entreprise pour chaque règle peut être différente d'une politique à l'autre.

En modifiant l'action découlant d'une règle, vous pouvez désactiver les règles qui vous donnent trop de faux-positifs, ou vous pouvez modifier si la règle alerte ou abandonne le trafic correspondant. Vous pouvez également activer des règles désactivées pour alerter ou abandonner le trafic correspondant.

La méthode la plus simple pour modifier les actions des règles est de modifier le niveau de sécurité d'un groupe de règles. Lorsque vous modifiez le niveau de sécurité d'un groupe, l'action des règles au sein du groupe change. Cela peut signifier que certaines règles sont activées (ou désactivées), ou que l'action peut

changer entre l'alerte et l'abandon, en fonction de l'état de sécurité que vous sélectionnez. Cependant, vous pouvez modifier une action découlant d'une règle individuelle si c'est ce dont vous avez besoin.

Remarque L'action par défaut pour une règle donnée est basée sur la sélection globale du groupe et de la gravité. La modification de la gravité du groupe ou l'exclusion du groupe peut modifier l'action par défaut de la règle.

Avant de commencer

Les groupes de règles personnalisées n'ont pas de niveau de sécurité. Vous ne pouvez pas utiliser la technique du niveau de sécurité pour modifier les actions découlant d'une règle pour des règles personnalisées.

Procédure

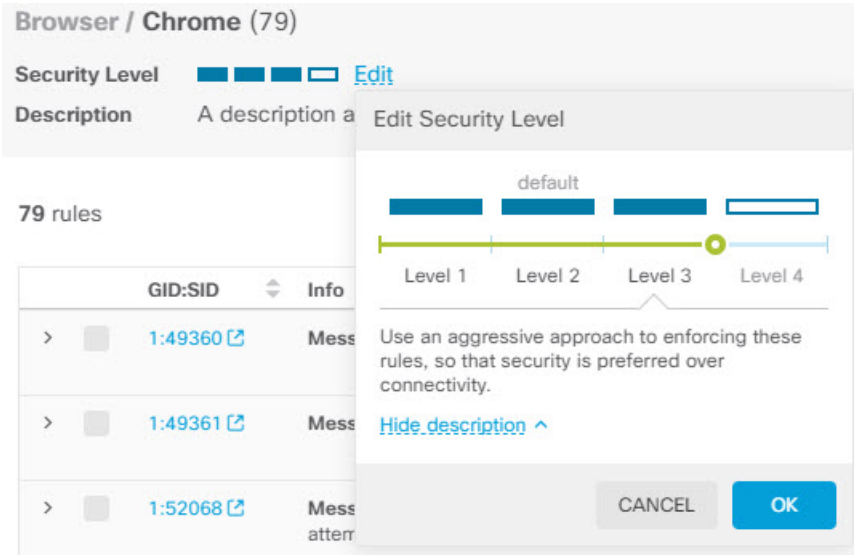
Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur l'icône Afficher ( ) de la politique dont vous souhaitez modifier les actions.

Étape 3 (Méthode recommandée.) Modifier le niveau de sécurité d'un groupe de règles.

a) Cliquez sur le groupe de règles enfant dans la liste des groupes de règles.

b) Au-dessus de la liste des règles, cliquez sur **Edit** (Modifier) à côté du niveau de sécurité du groupe.



Remarque
Si vous souhaitez désactiver toutes les règles du groupe, ne cliquez pas sur **Edit** (Modifier). Au lieu de cela, cliquez sur **Exclude** (Exclure) et confirmez que vous souhaitez exclure le groupe. Le groupe n'est pas supprimé, ses règles sont simplement désactivées. Ignorer les étapes restantes.

c) Sélectionnez le nouveau niveau pour le groupe. Cliquez sur **View Description** (Afficher la description) pour voir une explication de chaque niveau à mesure que vous le sélectionnez.

Le niveau 1 est la posture la moins sécurisée, car il met l'accent sur la connectivité plutôt que la sécurité, tandis que le niveau 4 est la posture la plus dynamique et offre une sécurité maximale.

d) Cliquez sur **OK**.

Étape 4 (Méthode manuelle.) Modifiez l'action pour une ou plusieurs règles.

a) Recherchez la règle dont vous souhaitez modifier l'action.

Utilisez la zone **Search/Filter** (rechercher/filtre) pour rechercher des chaînes dans les informations de règle. Vous pouvez également sélectionner des éléments de filtrage à rechercher sur n'importe quelle combinaison de GID ou SID, ou simplement afficher des règles en fonction de leurs actions (disabled (désactivé), alert (alerte), drop (abandon)). Les règles sont chargées au fur et à mesure, de sorte qu'il faut un certain temps pour faire défiler l'ensemble de la liste non filtrée. Lors du filtrage de la liste, cliquez sur le bouton Refresh (Actualiser) pour recharger l'affichage filtré.

Idéalement, vous pouvez obtenir l'identifiant Snort (SID) et l'identifiant de Générateur (GID) à partir d'un événement ou auprès de l'assistance technique de Cisco, si vous traitez un problème avec eux. Vous pouvez ensuite rechercher précisément la règle.

b) Pour modifier l'action, procédez comme suit :

- Modifier une règle à la fois : cliquez sur la colonne **Action** pour la règle et sélectionnez l'action requise :
  - **Alert** (Alerte) : ce choix crée un événement lorsque cette règle correspond au trafic, sans interrompre la connexion.
  - **Drop** (Abandon) : crée un événement lorsque cette règle correspond au trafic, puis interrompt la connexion.
  - **Disabled** (Désactivé) : ne correspond pas au trafic avec cette règle. Aucun événement n'est généré.
- Modifier plusieurs règles à la fois : cochez les cases des règles que vous souhaitez modifier, puis cliquez sur le menu déroulant **Bulk** au-dessus du tableau et choisissez l'action souhaitée. Cochez la case dans l'en-tête GID:SID pour sélectionner toutes les règles de la liste. Vous pouvez modifier jusqu'à 5 000 règles à la fois.

Gestion des règles de prévention des intrusions personnalisées et des groupes de règles

Le système est livré avec des règles de prévention des intrusions définies par Cisco Talos Intelligence Group (Talos). Si vous connaissez des attaques supplémentaires, vous pouvez créer et charger des règles de prévention des intrusions personnalisées pour filtrer ces attaques et les alerter ou les supprimer. Vous pouvez également créer, modifier et supprimer une règle à la fois.

Pour les règles chargées, vous créez les règles hors ligne à l'aide d'un éditeur de texte. Nous vous recommandons d'inclure un groupe de règles personnalisées dans chaque fichier texte que vous chargez. Vous pouvez ensuite facilement charger les modifications de vos règles et soit fusionner les nouvelles règles dans vos groupes de règles personnalisés, soit remplacer vos règles par des copies nouvelles et modifiées.

L'explication de la création de ces règles n'entre pas dans le cadre de ce document. Pour des informations détaillées sur la façon d'écrire des règles de prévention des intrusions pour Snort, y compris la conversion des règles Snort 2 au format Snort 3, consultez les guides sur https://snort.org/documents. Par exemple, *Règles*

d'introduction à l'écriture de règles Snort 3 à l'adresse https://snort.org/documents/rules-writers-guide-to-snort-3-rules.

Avant de commencer

Vous créez des groupes de règles personnalisés pendant le processus de chargement des règles personnalisées, comme décrit dans Chargement de règles de prévention des intrusions personnalisées, à la page 558, ou lors de la création de règles individuelles ou de la gestion de l'appartenance des règles. Après avoir créé le groupe, vous pouvez gérer le groupe et son contenu.

Notez que les groupes personnalisés sont disponibles pour toutes les politiques de prévention des intrusions, pas seulement pour la politique que vous modifiez lors de la création du groupe. Ainsi, les modifications que vous apportez à un groupe sont appliquées à toutes les politiques. Par exemple, si vous supprimez un groupe de règles personnalisées, il est supprimé de toutes les politiques et n'est plus disponible pour aucune d'entre elles.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur l'icône de modification ( ) d'une politique.

Nous vous recommandons d'ajouter des règles personnalisées à une politique de prévention des intrusions personnalisée plutôt qu'à l'une des politiques intégrées.

Étape 3 Effectuez l'une des actions suivantes :

- Pour créer un groupe, cliquez sur le signe plus **(+)** > **Upload Custom Rules** (Charger des règles personnalisées) . Consultez Chargement de règles de prévention des intrusions personnalisées, à la page 558.
- Pour modifier le nom ou la description d'un groupe, sélectionnez le groupe dans la table des matières du groupe dans le dossier Groupes définis par l'utilisateur. Vous pouvez ensuite cliquer sur **Edit** (Modifier) et apporter vos modifications.
- Pour exclure le groupe et ses règles de la politique, sélectionnez le groupe dans la table des matières du groupe dans le dossier Groupes définis par l'utilisateur. Vous pouvez ensuite cliquer sur **Exclude** (Exclure) pour supprimer le groupe.
- Pour supprimer le groupe du système et toutes les politiques qui l'utilisent, sélectionnez le groupe dans la table des matières du groupe dans le dossier Groupes définis par l'utilisateur. Cliquez sur **Delete** (Supprimer). Notez que si une règle n'existe que dans le groupe supprimé, elle est également supprimée du système. Toutefois, si une règle existe également dans d'autres groupes de règles personnalisées que vous ne supprimez pas, la règle reste dans ces groupes.
- Pour remplacer ou mettre à jour les règles d'un groupe en bloc, sélectionnez le groupe dans la table des matières du groupe dans le dossier Groupes définis par l'utilisateur. Ensuite, cliquez sur **Upload Rule File** (Charger le fichier de règles) à côté de la liste déroulante Action au-dessus du tableau de règles du groupe. Le processus est le même que celui décrit dans Chargement de règles de prévention des intrusions personnalisées, à la page 558.

- Pour créer et gérer des règles individuelles et leur affectation à des groupes de règles, consultez Configuration des règles de prévention des intrusions personnalisées individuelles, à la page 560.

Chargement de règles de prévention des intrusions personnalisées

Si vous connaissez des attaques qui ne sont actuellement pas couvertes par d'autres règles, vous pouvez créer et charger des règles de prévention des intrusions personnalisées pour filtrer ces attaques et générer une alerte ou abandonner le trafic. L'action des règles importées doit être « alert (alerte) » ou « drop (abandon) », et l'action par défaut de la règle est définie par l'action indiquée dans le fichier importé. Une fois importées, vous pouvez modifier l'action d'une règle et désactiver une règle au besoin.

Vous devez créer ces règles hors ligne. Dans cet écran Gestionnaire de périphériques de pare-feu, vous chargez simplement un fichier de règles ; vous ne configurez pas les règles directement. Le fichier de règles doit être un fichier texte. Vous pouvez utiliser des retours de ligne pour formater les règles afin qu'elles soient lisibles, ou placer une règle sur une seule ligne ; les lignes vides sont autorisées. Le format des règles est expliqué sur snort.org.

Par exemple, un fichier de chargement de trois règles peut ressembler à ce qui suit :

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (
   msg: "My Custom Rule: EXPLOIT-KIT Styx exploit kit landing page request";
   flow:to_server,established;
   http_raw_uri;
   bufferlen:>100;
   http_uri;
   content:"/i.html?",depth 8; pcre:"/\/i\.html\?[a-z0-9]+\=[a-zA-Z0-9]{25}/";
   flowbits:set,styx_landing;
   metadata: copied from talos sid 29452;
   service:http;
   classtype:trojan-activity;
   gid:1;
   sid:1000000;
   rev:1;
)

alert tcp $HOME_NET 8811 -> $EXTERNAL_NET any (
   msg:"My Custom rule: MALWARE-BACKDOOR fear1.5/aciddrop1.0 runtime detection - initial
connection";
   flow:to_client,established;
   flowbits:isset,Fear15_conn.2;
   content:"Drive",nocase;
   metadata:copied from talos sid 7710;
   classtype:trojan-activity;
   gid:1;
   sid:1000001;
   rev:1;
)

alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (
   msg:"My Custom Rule: INDICATOR-COMPROMISE download of a Office document with embedded
PowerShell";
   flow:to_client,established;
   flowbits:isset,file.doc;
   file_data;
   content:"powershell.exe",fast_pattern,nocase;
   metadata:copied from talos sid 37244;
   classtype:trojan-activity;
```

```
    gid:1;
    sid:1000002;
    rev:1;
)
```

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur l'icône de modification ( ) d'une politique.

Nous vous recommandons d'ajouter des règles personnalisées à une politique de prévention des intrusions personnalisée plutôt qu'à l'une des politiques intégrées.

Étape 3 Effectuez l'une des opérations suivantes :

- Au-dessus de la liste des groupes, cliquez sur **+** > **Upload Custom Rules** (Charger des règles personnalisées) .
- Si vous téléversez des règles dans un groupe de règles personnalisées que vous avez déjà créé, vous pouvez sélectionner le groupe de règles personnalisées, puis cliquer sur **Upload Rule File** (Charger le fichier de règles) à côté de la liste déroulante **Action** au-dessus du tableau de règles du groupe.

Étape 4 Cliquez sur **Browse** (Parcourir) et sélectionnez votre fichier de règle personnalisé, ou faites glisser le fichier et déposez-le dans la boîte de dialogue Upload File (Charger le fichier).

Attendez que le chargement soit terminé.

Étape 5 Sélectionnez la façon dont vous souhaitez gérer les conflits :

Il y a conflit lorsqu'une règle que vous ajoutez est identique à une règle déjà présente dans le système. Cela devrait se produire uniquement si vous téléversez les mêmes règles ou des versions modifiées de règles que vous avez déjà chargées.

Sélectionnez une des options :

Remarque
Les options **Merge** (Fusionner) et **Replace** (Remplacer) sont essentiellement la même chose. Les règles chargées doivent avoir des numéros de révision plus élevés que celles que vous avez déjà téléversées pour que des modifications soient apportées aux règles existantes. La seule différence est que si le fichier de chargement ne contient pas certaines règles présentes dans le groupe de règles personnalisées ciblé, l'option **Replace** (Remplacer) supprimera ces règles du groupe de règles. L'option **Merge** (Fusionner) laissera ces règles « manquantes » en place.

- **Merge** (Fusionner) : pour toute règle modifiée dans le fichier téléversé qui existe également dans le groupe sélectionné, ces modifications seront fusionnées si la règle dans le fichier téléversé a un numéro de révision plus élevé. Toutes les règles inchangées, ou les règles du groupe qui n'ont pas de règles correspondantes dans le téléversement, resteront inchangées. Toutes les nouvelles règles dans le chargement seront ajoutées. Il s'agit de l'option par défaut.
- **Replace** (Remplacer) : les règles dans le fichier chargé remplaceront les règles du groupe sélectionné si le numéro de révision de la règle chargée est supérieur. Toutes les règles existantes qui ne figurent pas dans le fichier chargé seront supprimées du groupe. Les règles existantes dont la version chargée a un numéro de révision identique ou inférieur resteront inchangées. Toutes les nouvelles règles dans le chargement seront ajoutées.

Étape 6 Cliquez sur + et sélectionnez le groupe de règles personnalisées pour les règles chargées.

Si le groupe de règles personnalisées que vous souhaitez utiliser n'existe pas encore, cliquez sur **Create New Group** (Créer un nouveau groupe) et créez-le maintenant. Le nouveau groupe a besoin d'un nom et, éventuellement, d'une description. Vous pouvez ensuite sélectionner le nouveau groupe.

Si vous remplacez des règles, vous ne pouvez sélectionner qu'un seul groupe. Si vous les fusionnez, vous pouvez sélectionner plusieurs groupes.

Étape 7 Cliquez sur **OK**.

Les fichiers sont chargés et placés dans le nouveau groupe. Vous devriez voir un résumé du nombre de règles qui ont été chargées et du nombre de règles mises à jour, supprimées ou ignorées.

S'il y a des erreurs dans le fichier, le chargement échouera. Vous pouvez cliquer sur le lien **Download Error File** (Télécharger le fichier d'erreurs) pour obtenir plus d'informations sur les erreurs.

Le groupe est automatiquement activé dans cette politique de prévention des intrusions. Le groupe et les nouvelles règles peuvent être ajoutés à d'autres politiques, mais le groupe et les règles ne sont automatiquement activés dans aucune autre politique. Pour en savoir plus sur l'ajout de groupes à d'autres politiques, consultez Ajout ou suppression de groupes de règles dans une politique de prévention des intrusions (Snort 3), à la page 553.

Configuration des règles de prévention des intrusions personnalisées individuelles

Vous pouvez configurer des règles de prévention des intrusions personnalisées une à la fois plutôt qu'en bloc par le biais du téléversement de fichiers. Cette méthode fonctionne bien lorsque vous devez effectuer un ajustement rapide à une règle ou que vous ne devez créer ou modifier que quelques règles à la fois.

Lors de la configuration des règles de prévention des intrusions, gardez les éléments suivants à l'esprit :

- Le GID de toutes les règles personnalisées doit être 1.
- Le SID d'une règle doit être unique pour toutes les règles du système. Il doit également être d'un million (1 000 000) ou plus.
- Si vous modifiez une règle, vous devez changer la version de la règle. Normalement, vous incrémentez le numéro de version de 1.
- Vous pouvez dupliquer une règle Cisco Talos Intelligence Group (Talos) pour créer votre propre version de la règle, mais vous devez toujours modifier le SID du doublon pour le rendre unique.

Le système effectuera des vérifications de validité pour s'assurer que la règle est bien formée, et vous verrez des messages d'erreur pour tout problème. Cependant, le système ne peut pas déterminer si la règle est sensible.

Pour des informations détaillées sur la façon d'écrire des règles de prévention des intrusions pour Snort, y compris la conversion des règles Snort 2 au format Snort 3, consultez les guides sur https://snort.org/documents. Par exemple, *Règles d'introduction à l'écriture de règles Snort 3* à l'adresse https://snort.org/documents/rules-writers-guide-to-snort-3-rules.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur l'icône de modification ( ) d'une politique.

Nous vous recommandons d'ajouter des règles personnalisées à une politique de prévention des intrusions personnalisée plutôt qu'à l'une des politiques intégrées.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour ajouter une règle de prévention des intrusions, cliquez sur le bouton **Add New Intrusion Rule** (Ajouter une nouvelle règle de prévention des intrusions) (+) au-dessus du tableau de règles. Lors de l'ajout d'une règle, vous devez sélectionner un ou plusieurs groupes de règles personnalisés pour contenir la nouvelle règle. Vous pouvez créer de nouveaux groupes tout en ajoutant la règle, au besoin.
- Pour ajouter une règle en dupliquant et en modifiant une règle existante, passez le curseur à l'extrémité droite de la règle, puis cliquez sur le bouton Duplicate (Dupliquer) ( ). Le bouton s'affiche uniquement lorsque vous passez le curseur. Pour les règles personnalisées, la commande **Duplicate** (Dupliquer) se trouve sous le bouton More Options (Plus d'options) (**...**).
- Pour modifier une règle personnalisée, recherchez la règle dans un groupe de règles personnalisées et cliquez sur le bouton de modification ( ) pour la règle. Vos modifications s'appliquent à tous les groupes dans lesquels la règle se trouve. Assurez-vous d'incrémenter le numéro de version de la règle d'au moins 1 lorsque vous apportez des modifications.
- Pour supprimer une règle personnalisée, cliquez sur le bouton de suppression ( ) correspondant à la règle. La règle est supprimée de tous les groupes de règles qui la contiennent. Si vous souhaitez simplement supprimer une règle d'un groupe, utilisez l'option **Manage Group Assignments** (Gérer les affectations de groupe) au lieu de supprimer la règle.
- Pour modifier les groupes qui contiennent la règle, cliquez sur le bouton More Options (Plus d'options) (**...**) et sélectionnez **Manage Group Assignments** (Gérer les affectations de groupe). Vous pouvez ensuite ajouter ou supprimer des groupes. Vos modifications affectent simplement l'appartenance au groupe, elles ne modifient pas la règle et ne la suppriment pas.

Étape 4 Pour les nouvelles règles et les groupes, ajoutez la règle à la politique.

Lorsque vous créez un nouveau groupe lors de la création d'une nouvelle règle ou de la modification d'une règle existante, ce groupe n'est pas ajouté automatiquement à votre politique et la règle n'est pas activée automatiquement. Vous êtes invité à ajouter le groupe à la politique que vous modifiez. Si vous n'ajoutez pas le groupe lors de l'ajout ou de la modification de la règle, vous pouvez ajouter le groupe ultérieurement en utilisant le processus suivant :

a) Cliquez sur + > **Add Existing Rule Group** (Ajouter un groupe de règles existant) au-dessus de la table des matières du groupe.
b) Recherchez le groupe dans le dossier User Defined Groups (Groupes définis par l'utilisateur), sélectionnez-le, puis cliquez sur **OK**.
c) Sélectionnez le groupe dans la table des matières et vérifiez que la nouvelle règle se trouve dans le groupe et comporte l'action souhaitée.

Gestion des politiques de prévention des intrusions (Snort 2)

Vous pouvez appliquer n'importe quelle politique de prévention des intrusions prédéfinie. Chacune de ces politiques comprend la même liste de règles de prévention des intrusions (également appelées signatures), mais elles varient dans les actions prises pour chaque règle. Par exemple, une règle peut être active dans une politique, mais désactivée dans une autre politique.

Si vous trouvez qu'une règle particulière vous donne trop de faux positifs, où la règle bloque le trafic que vous ne souhaitez pas bloquer, vous pouvez désactiver la règle sans avoir à passer à une politique de prévention des intrusions moins sécurisée. Vous pouvez également le modifier pour qu'il soit signalé par une alerte pour les correspondances sans perte du trafic.

Inversement, si vous savez que vous devez vous protéger contre une attaque spécifique, mais que la règle associée est désactivée dans la politique de prévention des intrusions de votre choix, vous pouvez activer la règle sans passer pour une politique plus sécurisée.

Utilisez les tableaux de bord liés aux intrusions et le Visualiseur d'événement (tous deux sur la page **Monitoring** (Surveillance)) pour évaluer l'incidence des règles de prévention des intrusions sur le trafic. Gardez à l'esprit que vous ne verrez les incidents d'intrusion et les données de prévention des intrusions que pour le trafic qui correspond aux règles de prévention des intrusions définies sur « alerte » ou « abandon »; les règles désactivées ne sont pas évaluées.

Les rubriques suivantes expliquent plus en détail les politiques de prévention des intrusions et le réglage des règles.

Configurer le mode d'inspection d'une politique de prévention des intrusions (Snort 2)

Par défaut, toutes les politiques de prévention des intrusions fonctionnent en mode de prévention pour mettre en œuvre un système de prévention des intrusions (IPS). En mode d'inspection de prévention, si une connexion correspond à une règle de prévention des intrusions dont l'action est d'abandonner le trafic, la connexion est activement bloquée.

Si vous souhaitez plutôt tester l'effet de la politique de prévention des intrusions sur votre réseau, vous pouvez passer au mode de détection, qui implémente un système de détection des intrusions (IDS). Dans ce mode d'inspection, les règles de rejet sont traitées comme des règles d'alerte, où vous êtes informé des connexions correspondantes, mais le résultat de l'action devient « aurait bloqué », et les connexions ne sont jamais bloquées.

Vous modifiez le mode d'inspection par politique de prévention des intrusions, de sorte que vous pouvez avoir une combinaison de prévention et de détection.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **Intrusion (Prévention des intrusions)**.

Étape 2 Cliquez sur l'onglet de la politique de prévention des intrusions dont vous souhaitez modifier le mode d'inspection.

Le **Inspection Mode** (Mode d'inspection) est indiqué au-dessus du tableau de règles.

Étape 3 Cliquez sur le lien **Edit (Modifier)** à côté du mode d'inspection, modifiez le mode pour la politique, puis cliquez sur **OK**.

Les options sont les suivantes :

- **Prevention** (Prévention) : les actions découlant d'une règle d'intrusion sont toujours appliquées. Les connexions correspondant à une règle de suppression sont bloquées.
- **Détection** : les règles d'intrusion génèrent uniquement des alertes. Une connexion qui correspond à une règle de suppression génère des messages d'alerte, mais la connexion n'est pas bloquée.

Modification des actions des règles de prévention des intrusions (Snort 2)

Chaque politique de prévention des intrusions prédéfinie comporte les mêmes règles. La différence est que l'action entreprise pour chaque règle peut être différente d'une politique à l'autre.

En modifiant l'action découlant d'une règle, vous pouvez désactiver les règles qui vous donnent trop de faux-positifs, ou vous pouvez modifier si la règle alerte ou abandonne le trafic correspondant. Vous pouvez également activer des règles désactivées pour alerter ou abandonner le trafic correspondant.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **Intrusion (Prévention des intrusions)**.

Étape 2 Cliquez sur l'onglet de la politique de prévention des intrusions dont vous souhaitez modifier les actions de règle.

Les politiques prédéfinies sont les suivantes :

- Connectivité avant la sécurité
- Sécurité et connectivité équilibrées
- Sécurité avant la connectivité
- Détection maximale

Étape 3 Recherchez la règle dont vous souhaitez modifier l'action.

Les règles sont triées en affichant d'abord celles qui ont été remplacées, puis par action au sein du groupe des règles remplacées. Sinon, les règles sont triées par GID, puis par SID.

Utilisez la zone de recherche pour localiser la règle que vous souhaitez modifier. Idéalement, vous pouvez obtenir l'identifiant Snort (SID) et l'identifiant de Générateur (GID) à partir d'un événement ou auprès de l'assistance technique de Cisco, si vous traitez un problème avec eux.

Pour des informations détaillées sur les éléments de chaque règle, consultez Attributs des règles d'intrusion, à la page 541.

Pour effectuer une recherche dans la liste :

a) Cliquez dans la zone **Search** (Rechercher) pour ouvrir la boîte de dialogue des attributs de recherche.

b) Saisissez une combinaison d'ID de Générateur (**GID**), d'ID Snort (**SID**) ou **d'action** de règle, puis cliquez sur **Search** (Rechercher).

Par exemple, vous pourriez sélectionner **Action = Drop** pour voir toutes les règles de la politique qui bloqueront les connexions correspondantes. Le texte à côté de la zone de recherche indique le nombre de règles correspondant à vos critères, par exemple, « 8937 sur 9416 règles trouvées ».

Pour effacer un critère de recherche, cliquez sur le x pour le critère dans la zone de recherche.

Étape 4 Cliquez sur la colonne **Action** pour la règle et sélectionnez l'action requise :

- **Alert** (Alerte) : ce choix crée un événement lorsque cette règle correspond au trafic, sans interrompre la connexion.
- **Drop** (Abandon) : crée un événement lorsque cette règle correspond au trafic, puis interrompt la connexion.
- **Disabled** (Désactivé) : ne correspond pas au trafic avec cette règle. Aucun événement n'est généré.

L'action par défaut de la règle est indiquée par « (Default) » ajouté à l'action. Si vous modifiez la valeur par défaut, la colonne d'état indique « Overridden » (Remplacer) pour cette règle.

Surveillance des politiques de prévention des intrusions

Vous pouvez trouver les statistiques de politique de prévention des intrusions dans les tableaux de bord **Attackers** (attaquants) et **Targets** (cibles) sur la page **Monitoring** (surveillance). Vous devez appliquer une politique de prévention des intrusions à au moins une règle de contrôle d'accès pour voir des informations dans ces tableaux de bord. Consultez Tableaux de bord du trafic et du système, à la page 108.

Pour voir les incidents d'intrusion, sélectionnez **Monitoring (Surveillance)** > **Events (Événements**, puis cliquez sur l'onglet **Intrusion**. Vous pouvez placer le curseur sur un événement et cliquer sur le lien **View Details** (afficher les détails) pour obtenir plus d'informations. Dans la page des détails, vous pouvez cliquer sur **View IPS Rule** (afficher la règle IPS) pour accéder à la règle dans la politique de prévention des intrusions appropriée, où vous pouvez modifier l'action associée à la règle. Cela peut vous aider à réduire l'impact des faux positifs, lorsqu'une règle bloque trop de bonnes connexions, en modifiant l'action de drop (abandon) à alert (alerte). Inversement, vous pouvez transformer une règle d'alerte (alert rule) en règle de rejet (drop rule) si vous voyez beaucoup de trafic d'attaque pour une règle.

Si vous configurez un serveur syslog pour la politique de prévention des intrusions, les incidents d'intrusion ont l'ID de message 430001.

Exemples de politiques de prévention des intrusions

Le chapitre sur les intrusions comprend les exemples suivants de mise en œuvre des politiques de prévention des intrusions.

- Comment bloquer les menaces, à la page 56
- Comment surveiller passivement le trafic sur un réseau, à la page 78



CHAPITRE 23

Traduction d'adresses réseau (NAT)

Les rubriques suivantes expliquent la traduction d'adresses réseau (NAT) et comment la configurer sur le périphérique.

- Pourquoi utiliser la NAT?, à la page 565
- Principes de base de la NAT, à la page 566
- Directives pour la NAT, à la page 573
- Configurer la traduction d'adresses réseau (NAT), à la page 578
- Traduction de réseaux IPv6, à la page 607
- Surveillance de la NAT, à la page 621
- Exemples relatifs à la NAT, à la page 622

Pourquoi utiliser la NAT?

Chaque ordinateur et périphérique d'un réseau IP reçoit une adresse IP unique qui permet d'identifier l'hôte. En raison d'une pénurie d'adresses IPv4 publiques, la plupart de ces adresses IP sont privées et ne peuvent être routées nulle part en dehors du réseau privé de l'entreprise. RFC 1918 définit les adresses IP privées que vous pouvez utiliser en interne et qui ne doivent pas être annoncées :

- 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

L'une des principales fonctions de la NAT est de permettre aux réseaux IP privés de se connecter à Internet. La NAT remplace une adresse IP privée par une adresse IP publique, en transformant les adresses privées du réseau privé interne en adresses légales et routables qui peuvent être utilisées sur l'Internet public. De cette façon, la NAT conserve les adresses publiques, car elle peut être configurée pour annoncer au moins une adresse publique pour l'ensemble du réseau vers le monde extérieur.

Les autres fonctions de la NAT comprennent :

- Sécurité : le fait de garder les adresses IP internes masquées détourne les attaques directes.
- Solutions de routage IP : les adresses IP qui se chevauchent ne sont pas un problème lorsque vous utilisez la NAT.

- Souplesse : vous pouvez modifier les schémas d'adressages IP internes sans affecter les adresses publiques disponibles en externe. par exemple, pour un serveur accessible à Internet, vous pouvez conserver une adresse IP fixe pour l'utilisation d'Internet, mais à l'interne, vous pouvez modifier l'adresse du serveur.
- Traduction entre IPv4 et IPv6 (mode routage uniquement) Si vous souhaitez connecter un réseau IPv6 à un réseau IPv4, la NAT vous permet de traduire entre les deux types d'adresses.



Remarque La NAT n'est pas requise. Si vous ne configurez pas la NAT pour un ensemble donné de trafic, ce trafic ne sera pas traduit, mais toutes les politiques de sécurité seront appliquées normalement.

Principes de base de la NAT

Les rubriques suivantes expliquent certains des principes de base de la NAT.

Terminologie NAT

Le présent document utilise les termes suivants :

- Real address/host/network/interface : L'adresse réelle est l'adresse définie sur l'hôte avant qu'elle ne soit traduite. Dans un scénario NAT typique, vous souhaitez traduire le réseau interne lorsqu'il accède à l'extérieur, le réseau interne serait le « vrai » réseau. Notez que vous pouvez traduire n'importe quel réseau connecté au périphérique, pas seulement un réseau interne. Par conséquent, si vous configurez la NAT pour traduire les adresses externes, « réel » peut faire référence au réseau externe lorsqu'il accède au réseau interne.
- Mapped address/host/network/interface (adresse/hôte/réseau/interface mappée) : l'adresse mappée est l'adresse dans laquelle l'adresse réelle est traduite. Dans un scénario NAT typique, où vous souhaitez traduire le réseau interne lorsqu'il accède à l'extérieur, le réseau externe serait le réseau « mappé ».



Remarque Pendant la traduction d'adresses, les adresses IP configurées pour les interfaces de périphérique ne sont pas traduites.

- Lancement bidirectionnel : la NAT statique permet aux connexions d'être lancées de façon *bidirectionnelle*, c'est-à-dire à la fois vers l'hôte et à partir de l'hôte.
- NAT de source et de destination : pour tout paquet donné, les adresses IP de source et de destination sont comparées aux règles de la NAT, et l'une d'elles ou les deux peuvent être traduites ou non traduites, selon le cas. Pour la NAT statique, la règle est bidirectionnelle, il faut donc savoir que les termes « source » et « destination » sont utilisés dans les commandes et les descriptions tout au long de ce guide, même si une connexion donnée peut provenir de l'adresse de « destination ».

Types de NAT

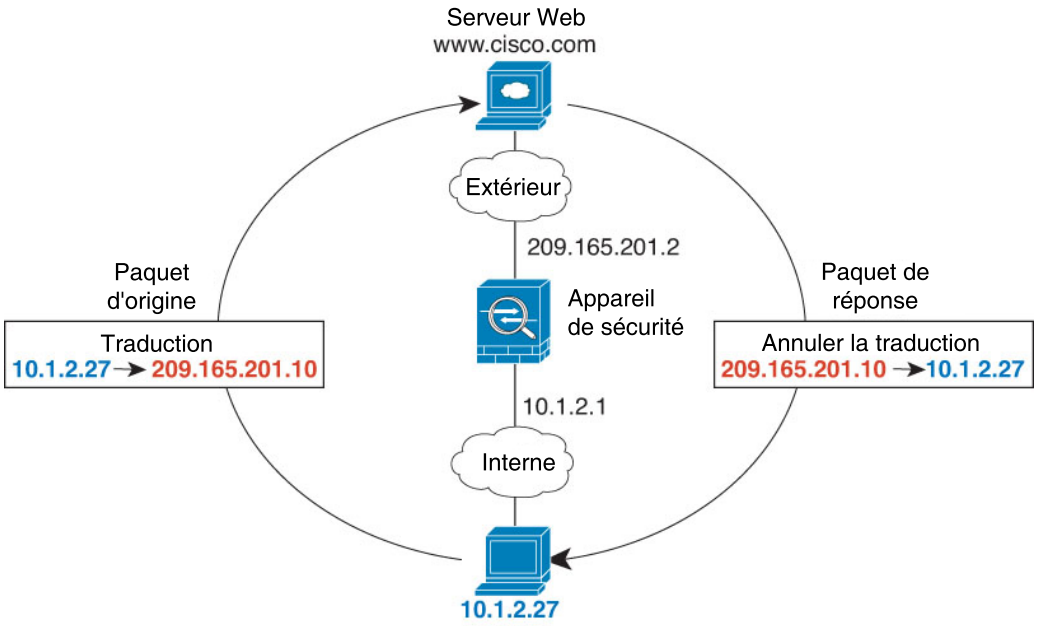
Vous pouvez implémenter la NAT en utilisant les méthodes suivantes :

- NAT dynamique : un groupe d'adresses IP réelles est mappé à un groupe (généralement plus petit) d'adresses IP mappées, selon le principe du premier arrivé, premier servi. Seul l'hôte réel peut initier le trafic. Consultez Traduction d'adresses réseau dynamique, à la page 579.
- Traduction dynamique des adresses de port (PAT) : un groupe d'adresses IP réelles est mappé à une adresse IP unique en utilisant un port source unique de cette adresse IP. Consultez PAT dynamique, à la page 584.
- NAT statique : un mappage cohérent entre une adresse IP réelle et une adresse IP mappée. Autorise le lancement de trafic bidirectionnel. Consultez NAT statique, à la page 589.
- NAT d'identité : une adresse réelle est traduite statiquement en elle-même, contournant essentiellement la NAT. Vous pourriez souhaiter configurer la NAT de cette façon lorsque vous souhaitez traduire un grand groupe d'adresses, mais que vous souhaitez ensuite exempter un plus petit sous-ensemble d'adresses. Consultez NAT d'identité, à la page 598.

NAT en mode routé

La figure suivante montre un exemple de NAT typique en mode routé, avec un réseau privé à l'intérieur.

Illustration 9 : Exemple de NAT : mode routé



1. Lorsque l'hôte interne en 10.1.2.27 envoie un paquet à un serveur Web, l'adresse source réelle du paquet, 10.1.2.27, est convertie en une adresse mappée, 209.165.201.10.
2. Lorsque le serveur répond, il envoie la réponse à l'adresse mappée, 209.165.201.10, et l' Appareil FTD reçoit le paquet, car l' Appareil FTD effectue un ARP mandataire pour réclamer le paquet.
3. L' Appareil FTD remplace ensuite la traduction de l'adresse mappée, 209.165.201.10, par l'adresse réelle, 10.1.2.27, avant de l'envoyer à l'hôte.

NAT automatique et NAT manuelle

Vous pouvez mettre en œuvre la traduction d'adresses de deux manières : *auto NAT* et *NAT manuelle*.

Nous vous recommandons d'utiliser l'auto NAT, sauf si vous avez besoin des fonctionnalités supplémentaires offertes par NAT manuelle. Il est plus facile de configurer auto NAT et ce pourrait être plus fiable pour des applications telles que la voix sur IP (VoIP). (Pour la VoIP, vous pourriez constater un échec dans la traduction des adresses indirectes qui n'appartiennent à aucun des objets utilisés dans la règle.)

NAT automatique

Toutes les règles NAT configurées comme paramètre d'un objet réseau sont considérées comme des règles *auto NAT*. Il s'agit d'un moyen rapide et simple de configurer la NAT pour un objet réseau. Vous ne pouvez pas créer ces règles pour un objet de groupe, cependant.

Bien que ces règles soient configurées dans le cadre de l'objet lui-même, vous ne pouvez pas afficher la configuration NAT dans la définition de l'objet par le biais du gestionnaire d'objets.

Lorsqu'un paquet entre dans une interface, les adresses IP de source et de destination sont vérifiées par rapport aux règles auto NAT. Les adresses de source et de destination du paquet peuvent être traduites par des règles distinctes si des correspondances distinctes sont effectuées. Ces règles ne sont pas liées les unes aux autres; Différentes combinaisons de règles peuvent être utilisées en fonction du trafic.

Comme les règles ne sont jamais jumelées, vous ne pouvez pas préciser que sourceA/destinationA doit avoir une traduction différente de celle de sourceA/destinationB. Utilisez NAT manuelle pour ce type de fonctionnalité, où vous pouvez identifier l'adresse de source et de destination dans une seule règle.

NAT manuelle

La NAT manuelle vous permet d'identifier l'adresse source et l'adresse de destination en une seule règle. Préciser les adresses de source et de destination vous permet de préciser que sourceA/destinationA peut avoir une traduction différente de celle de sourceA/destinationB.



Remarque Pour la NAT statique, la règle est bidirectionnelle, il faut donc savoir que les termes « source » et « destination » sont utilisés dans les commandes et les descriptions tout au long de ce guide, même si une connexion donnée peut provenir de l'adresse de « destination ». Par exemple, si vous configurez la NAT statique avec traduction d'adresse de port et spécifiez l'adresse source comme une adresse de serveur Telnet, et que vous souhaitez que tout le trafic allant vers ce serveur Telnet ait le port traduit de 2323 à 23, vous devez spécifier les ports *source* à traduire (réel : 23, mappé : 2323). Vous spécifiez les ports source, car vous avez spécifié l'adresse du serveur Telnet comme adresse source.

L'adresse de destination est facultative. Si vous spécifiez l'adresse de destination, vous pouvez soit la mapper avec elle-même (NAT d'identité), soit la mapper avec une adresse différente. Le mappage de destination est toujours un mappage statique.

Comparaison de la NAT automatique et la NAT manuelle

Les principales différences entre ces deux types de NAT sont les suivantes :

- Votre définition de l'adresse réelle.
    - NAT automatique : la règle NAT devient un paramètre pour un objet réseau. L'adresse IP de l'objet réseau sert d'adresse (réelle) d'origine.

- NAT manuelle : vous identifiez un objet réseau ou un groupe d'objets réseau pour les adresses réelles et mappées. Dans ce cas, la NAT n'est pas un paramètre de l'objet réseau; l'objet ou le groupe de réseau est un paramètre de la configuration NAT. La possibilité d'utiliser un *groupe* d'objets réseau pour l'adresse réelle signifie que NAT manuelle est plus évolutif.

- Mise en œuvre de la NAT de source et de destination.
  - NAT automatique : chaque règle peut s'appliquer à la source ou à la destination d'un paquet. Deux règles peuvent donc être utilisées, une pour l'adresse IP source et une pour l'adresse IP de destination. Ces deux règles ne peuvent pas être liées ensemble pour appliquer une traduction précise pour une combinaison source/destination.
  - NAT manuelle : une règle unique traduit à la fois la source et la destination. Un paquet correspond à une seule règle et les autres règles ne sont pas vérifiées. Même si vous ne configurez pas l'adresse de destination facultative, un paquet correspondant correspond toujours à une seule règle NAT manuelle. La source et la destination sont liées, vous pouvez donc appliquer différentes traductions selon la combinaison source/destination. Par exemple, sourceA/destinationA peut avoir une traduction différente de sourceA/destinationB.

- Ordre des règles NAT
  - NAT automatique : classés automatiquement dans la table NAT.
  - NAT manuelle : classés manuellement dans la table NAT (avant ou après les règles auto NAT).

Ordre des règles NAT

Les règlesNAT automatique et NAT manuelle sont stockées dans un seul tableau qui est divisé en trois sections. Les règles de la section 1 sont appliquées en premier, puis les règles de la section 2 et finalement de la section 3 jusqu'à ce qu'une correspondance soit trouvée. Par exemple, si une correspondance est trouvée dans la section 1, les sections 2 et 3 ne sont pas évaluées. Le tableau suivant montre l'ordre des règles dans chaque section.



Remarque Il existe également une section 0, qui contient toutes les règles NAT créées par le système pour son propre usage. Ces règles ont priorité sur toutes les autres. Le système crée automatiquement ces règles et efface les xlates si nécessaire. Vous ne pouvez pas ajouter, modifier ni modifier les règles de la section 0.

Tableau 13 : Tableau des règles NAT.

Section de tableau	Type de règle	Ordre des règles dans la section
Section 1	NAT manuelle	Appliqués lors de la première correspondance, dans l'ordre dans lequel elles apparaissent dans la configuration. Étant donné que la première correspondance est appliquée, vous devez vous assurer que les règles spécifiques précèdent les règles plus générales, sans quoi les règles spécifiques pourraient ne pas être appliquées comme vous le souhaitez. Par défaut, les règles NAT manuelle sont ajoutées à la section 1. Par « les règles spécifiques d'abord », nous entendons : • Les règles statiques doivent précéder les règles dynamiques. • Les règles qui incluent la traduction de destination doivent être placées avant les règles ne comprenant que la traduction de la source. Si vous ne pouvez pas éliminer les règles en chevauchement, lorsque plusieurs règles peuvent s'appliquer en fonction de l'adresse source ou de destination, soyez particulièrement prudent en suivant ces recommandations.
Section 2	NAT automatique	Si aucune correspondance n'est trouvée dans la section 1, les règles de la section 2 sont appliquées dans l'ordre suivant : **1.** Règles statiques. **2.** Règles dynamiques. **Pour chaque type de règle, les consignes d'ordre suivantes sont utilisées :** **1.** Quantité d'adresses IP réelles : de la plus petite à la plus grande. Par exemple, un objet avec une adresse sera évalué avant un objet avec 10 adresses. **2.** Pour les quantités identiques, l'adresse IP du numéro est utilisée, du plus bas au plus élevé. Par exemple, 10.1.1.0 est évaluée avant 11.1.1.0. **3.** Si la même adresse IP est utilisée, le nom de l'objet réseau est utilisé, par ordre alphabétique. Par exemple, abracadabra est évalué avant catwoman.
Section 3	NAT manuelle	Si aucune correspondance n'est trouvée, les règles de la section 3 sont appliquées selon la première correspondance, dans l'ordre dans lequel elles apparaissent dans la configuration. Cette section devrait contenir vos règles les plus générales. Vous devez également vous assurer que toutes les règles spécifiques de cette section précèdent les règles générales qui s'appliqueraient autrement.

Pour les règles de la section 2, par exemple, les adresses IP suivantes sont définies dans les objets réseau :

- 192.168.1.0/24 (statique)
- 192.168.1.0/24 (dynamique)
- 10.1.1.0/24 (statique)
- 192.168.1.1/32 (statique)
- 172.16.1.0/24 (dynamique) (définition de l'objet)
- 172.16.1.0/24 (dynamique) (objet abc)

L'ordre résultant serait le suivant :

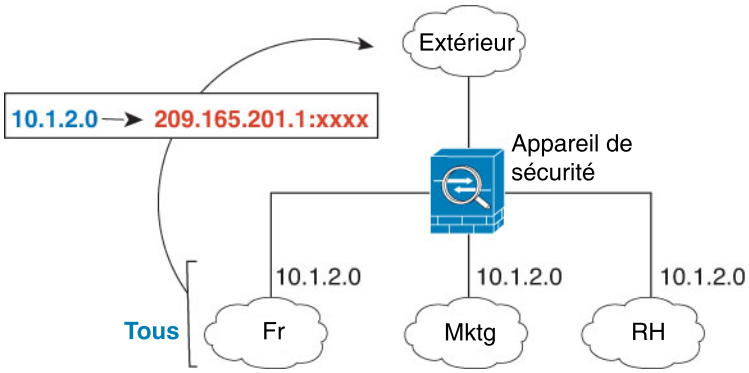
- 192.168.1.1/32 (statique)
- 10.1.1.0/24 (statique)
- 192.168.1.0/24 (statique)
- 172.16.1.0/24 (dynamique) (objet abc)
- 172.16.1.0/24 (dynamique) (définition de l'objet)
- 192.168.1.0/24 (dynamique)

Interfaces NAT

À l'exception des interfaces membres des groupes de ponts, vous pouvez configurer une règle NAT à appliquer à n'importe quelle interface (c'est-à-dire à toutes les interfaces) ou vous pouvez identifier des interfaces réelles et mappées spécifiques. Vous pouvez également spécifier n'importe quelle interface pour l'adresse réelle et une interface particulière pour l'adresse mappée, ou inversement.

Par exemple, vous pourriez souhaiter spécifier n'importe quelle interface pour l'adresse réelle et spécifier l'interface externe pour l'adresse mappée si vous utilisez les mêmes adresses privées sur plusieurs interfaces et que vous souhaitez les traduire toutes vers le même ensemble global lors de l'accès à .

Illustration 10 : Spécification d'une interface



Cependant, le concept d'interface « quelconque » (any) ne s'applique pas aux interfaces des membres des groupes de ponts. Lorsque vous spécifiez une interface « any », toutes les interfaces des membres des groupes de ponts sont exclues. Ainsi, pour appliquer la NAT aux membres du groupe de ponts, vous devez préciser

l'interface membre. Il peut en résulter de nombreuses règles similaires où une seule interface est différente. Vous ne pouvez pas configurer la NAT pour l'interface virtuelle de pont (BVI) elle-même, vous pouvez configurer la NAT pour les interfaces membres uniquement.



Remarque Vous ne pouvez pas configurer la NAT pour les interfaces fonctionnant en modes en ligne, en mode Tap sur la ligne ou passif. Lorsque vous spécifiez des interfaces, vous le faites indirectement en sélectionnant l'objet d'interface qui contient l'interface.

Configurer le routage pour la NAT

Le périphérique Firepower Threat Defense doit être la destination de tous les paquets envoyés à l'adresse traduite (mappée).

Lors de l'envoi de paquets, le périphérique utilise l'interface de destination si vous en spécifiez une, ou une recherche dans la table de routage si vous n'en spécifiez pas, pour déterminer l'interface de sortie. Pour la NAT d'identité, vous avez la possibilité d'utiliser une recherche de route même si vous spécifiez une interface de destination.

Le type de configuration de routage nécessaire dépend du type d'adresse mappée, comme expliqué dans les rubriques suivantes.

Adresses sur le même réseau que l'interface mappée

Si vous utilisez des adresses sur le même réseau que l'interface mappée, l' Appareil FTDutilise un serveur mandataire ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car Appareil FTD n'a pas à constituer la passerelle pour d'autres réseaux. Cette solution est idéale si le réseau externe contient un nombre adéquat d'adresses libres, une considération si vous utilisez une traduction 1:1 comme la NAT dynamique ou statique. La PAT dynamique étend considérablement le nombre de traductions que vous pouvez utiliser avec un petit nombre d'adresses. Ainsi, même si les adresses disponibles sur le réseau externe sont petites, cette méthode peut être utilisée. Pour PAT, vous pouvez même utiliser l'adresse IP de l'interface mappée.

Adresses sur un réseau unique

Si vous avez besoin de plus d'adresses qu'il n'y en a sur le réseau d'interface de destination (mappé), vous pouvez identifier les adresses sur un autre sous-réseau. Le routeur en amont a besoin d'une route statique pour les adresses mappées qui pointe vers Appareil FTD.

Même adresse que l'adresse réelle (NAT d'identité)

Dans le comportement par défaut de la NAT d'identité, le mandataire ARP est activé, ce qui correspond aux autres règles NAT statiques. Vous pouvez désactiver le mandataire ARP si vous le souhaitez. Vous pouvez également désactiver le mandataire ARP pour la NAT statique normale si vous le souhaitez, auquel cas vous devez vous assurer d'avoir les routages appropriés sur le routeur en amont.

Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité. Par exemple, si vous configurez une règle NAT d'identité large pour « n'importe quelle » adresse IP, laisser le mandataire ARP activé peut entraîner des problèmes pour les hôtes du réseau directement connectés à l'interface mappée. Dans ce cas, quand un hôte sur le réseau mappé souhaite communiquer avec un autre hôte sur le même réseau, l'adresse de la demande ARP correspond à la

règle NAT (qui correspond à « n'importe quelle » adresse). L' Appareil FTD fera ensuite passer l'ARP par un serveur mandataire pour l'adresse, même si le paquet n'est pas réellement destiné à Appareil FTD. (Notez que ce problème se produit même si vous avez une règle NAT manuelle ; bien que la règle NAT doive correspondre aux adresses source et de destination, la décision du protocole ARP est prise uniquement en fonction de l'adresse « source »). Si la réponse ARP Appareil FTD est reçue avant la réponse effective ARP de l'hôte, le trafic sera envoyé par erreur vers Appareil FTD.

Directives pour la NAT

Les rubriques suivantes fournissent des instructions détaillées pour la mise en œuvre de la NAT.

Directives relatives à l'interface

La NAT est prise en charge pour les interfaces physiques ou les sous-interfaces routées standard.

Cependant, la configuration de la NAT sur des interfaces membres d'un groupe de pont (interfaces faisant partie d'une Bridge Virtual Interface, ou BVI) est soumise aux restrictions suivantes :

- Lors de la configuration de la NAT pour les membres d'un groupe de ponts, vous spécifiez l'interface membre. Vous ne pouvez pas configurer la NAT pour l'interface de groupe de ponts (BVI) elle-même.
- Lorsque vous effectuez la NAT entre des interfaces membres d'un groupe de pont, vous devez préciser les interfaces source et de destination. Vous ne pouvez pas définir « any » comme interface.
- Vous ne pouvez pas configurer la PAT d'interface lorsque l'interface de destination est une interface membre d'un groupe de pont, car aucune adresse IP n'est associée à l'interface.
- Vous ne pouvez pas traduire entre les réseaux IPv4 et IPv6 (NAT64/46) lorsque les interfaces de source et de destination sont membres du même groupe de ponts. La NAT statique/PAT 44/66, la NAT dynamique 44/66 et la PAT 44 dynamique sont les seules méthodes autorisées; La PAT 66 dynamique n'est pas pris en charge.

Directives pour la NAT pour IPv6

La NAT prend en charge IPv6 avec les directives et restrictions suivantes.

- Pour les interfaces en mode routé standard, vous pouvez également traduire entre IPv4 et IPv6.
- Vous ne pouvez pas traduire entre IPv4 et IPv6 pour des interfaces qui sont membres du même groupe de pont. Vous pouvez uniquement traduire entre deux réseaux IPv6 ou deux réseaux IPv4. Cette restriction ne s'applique pas lorsque les interfaces sont membres de différents groupes de ponts ou entre un membre de groupe de ponts et une interface de routage standard.
- Vous ne pouvez pas utiliser la PAT dynamique pour IPv6 (NAT66) lors de la traduction entre les interfaces du même groupe de ponts. Cette restriction ne s'applique pas lorsque les interfaces sont membres de différents groupes de ponts ou entre un membre de groupe de ponts et une interface de routage standard.
- Pour la NAT statique, vous pouvez spécifier un sous-réseau IPv6 jusqu'à /64. Les sous-réseaux plus importants ne sont pas pris en charge.

- Lors de l'utilisation de FTP avec NAT46, lorsqu'un client FTP pour IPv4 se connecte à un serveur FTP pour IPv6, le client doit utiliser le mode passif étendu (EPSV), ou le mode Port étendu (EPRT); Les commandes PASV et PORT ne sont pas prises en charge avec IPv6.

Bonnes pratiques pour la NAT IPv6

Vous pouvez utiliser la NAT pour traduire entre des réseaux IPv6, mais aussi entre des réseaux IPv4 et IPv6 (mode routage uniquement). Nous recommandons les bonnes pratiques suivantes :

- NAT66 (IPv6-vers-IPv6) : nous vous recommandons d'utiliser une NAT statique. Bien que vous puissiez utiliser la NAT ou la PAT dynamique, les adresses IPv6 sont si nombreuses que vous n'êtes pas obligé d'utiliser la NAT dynamique. Si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle (NAT manuelle uniquement).
- NAT46 (IPv4-vers-IPv6) : nous vous recommandons d'utiliser une NAT statique. Étant donné que l'espace d'adresse IPv6 est beaucoup plus important que l'espace d'adresse IPv4, vous pouvez facilement réaliser une traduction statique. Si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle (NAT manuelle uniquement). Lors de la traduction vers un sous-réseau IPv6 (/96 ou inférieur), l'adresse mappée résultante est par défaut une adresse IPv4 intégrée, où les 32 bits de l'adresse IPv4 sont intégrés après le préfixe IPv6. Par exemple, si le préfixe IPv6 est un préfixe /96, l'adresse IPv4 est ajoutée dans les 32 derniers bits de l'adresse. Par exemple, si vous mappez 192.168.1.0/24 à 201b::0/96, 192.168.1.4 sera mappé à 201b::0.192.168.1.4 (affichée avec une notation mixte). Si le préfixe est inférieur, comme /64, l'adresse IPv4 est ajoutée après le préfixe et un suffixe 0s est ajouté après l'adresse IPv4.
- NAT64 (IPv6-vers-IPv4) : il se peut que vous n'ayez pas assez d'adresses IPv4 pour le nombre d'adresses IPv6. Nous vous recommandons d'utiliser un ensemble PAT dynamique pour fournir un grand nombre de traductions IPv4.

Prise en charge de la NAT pour les protocoles inspectés

Certains protocoles de couche d'application qui ouvrent des connexions secondaires ou qui intègrent des adresses IP dans les paquets sont inspectés pour fournir les services suivants :

- Pinhole création (création d'orifices) : certains protocoles d'application ouvrent des connexions TCP ou UDP secondaires sur des ports standard ou négociés. L'inspection ouvre des pinholes pour ces ports secondaires, vous n'avez donc pas besoin de créer des règles de contrôle d'accès pour les autoriser.
- Réécriture NAT : Les protocoles tels que le FTP intègrent les adresses IP et les ports pour les connexions secondaires dans les paquets de données dans le cadre du protocole. Si une traduction NAT est impliquée pour l'un ou l'autre des points terminaux, les moteurs d'inspection réécrivent les données du paquet pour refléter la traduction NAT des adresses et des ports intégrés. Les connexions secondaires ne fonctionneraient pas sans la réécriture de la NAT.
- Application de protocole : certaines inspections appliquent un certain degré de conformité aux RFC pour le protocole inspecté.

Le tableau suivant répertorie les protocoles inspectés qui appliquent la réécriture NAT et leurs limites NAT. Gardez ces limitations à l'esprit lors de l'écriture de règles NAT qui incluent ces protocoles. Les protocoles inspectés qui ne sont pas répertoriés ici n'appliquent pas la réécriture NAT. Ces inspections comprennent GTP, HTTP, IMAP, POP, SMTP, SSH et SSL.

Remarque La réécriture de la NAT est prise en charge sur les ports répertoriés uniquement. Si vous utilisez ces protocoles sur des ports non standard, n'utilisez pas la NAT sur les connexions.

Tableau 14 : Inspection des applications NAT prises en charge

Application	Protocole inspecté, port	Limites de la NAT	Pinholes créés
DCERPC	TCP/135	No NAT64.	Oui
DNS sur UDP	UDP/53	Aucune prise en charge de NAT n'est disponible pour la résolution de nom par le biais de WINS.	Non
ESMTP	TCP/25	No NAT64.	Non
FTP	TCP/21	Aucune restriction.	Oui
H.323 H.225 (signalisation d'appel) H.323 RAS	TCP/1720 UDP/1718 Pour ARS, UDP/1718-1719	No NAT64.	Oui
ICMP Erreur ICMP	ICMP (Le trafic ICMP dirigé vers une interface de périphérique n'est jamais inspecté.)	Aucune restriction.	Non
Options d'adresse IP	RSVP	No NAT64.	Non
Serveur de noms NetBIOS sur IP	UDP/133, 138 (ports sources)	No NAT64.	Non
RSH	TCP/514	Pas de PAT No NAT64.	Oui
RTSP	TCP/554 (Aucun traitement pour la masquage HTTP.)	No NAT64.	Oui
SIP	TCP/5060 UDP/5060	Pas de PAT étendue. Pas de NAT64 ou NAT46.	Oui
Skinny (SCCP)	TCP/2000	Pas de NAT64, NAT46 ou NAT66.	Oui
SQL*Net (versions 1, 2)	TCP/1521	No NAT64.	Oui

Application	Protocole inspecté, port	Limites de la NAT	Pinholes créés
Sun RPC	TCP/111 UDP/111	No NAT64.	Oui
TFTP	UDP/69	No NAT64. Les adresses IP de charge utile ne sont pas traduites.	Oui
XDMCP	UDP/177	No NAT64.	Oui

Directives supplémentaires pour la NAT

- Les règles NAT s'appliquent uniquement au trafic du périphérique. Elles ne s'appliquent pas au trafic initié par le périphérique, comme une authentification RADIUS.
- Pour les interfaces membres d'un groupe de ponts, vous écrivez les règles NAT pour les interfaces membres. Vous ne pouvez pas écrire de règles NAT pour l'interface virtuelle de pont (BVI) elle-même.
- Vous ne pouvez pas écrire de règles NAT pour les interfaces de tunnel virtuel (VTI), qui sont utilisées dans le VPN de site à site. L'écriture de règles pour l'interface source du VTI n'appliquera pas la NAT au tunnel VPN. Pour écrire des règles NAT qui s'appliqueront au trafic VPN acheminé par tunnellisation sur un VTI, vous devez utiliser « any » comme interface; vous ne pouvez pas spécifier explicitement les noms d'interface.
- (NAT automatique seulement.) Vous ne pouvez définir qu'une seule règle NAT pour un objet donné; si vous souhaitez configurer plusieurs règles NAT pour un objet, vous devez créer plusieurs objets avec des noms différents qui spécifient la même adresse IP.
- Si un VPN est défini sur une interface, le trafic ESP entrant sur l'interface n'est pas soumis aux règles de la NAT. Le système autorise le trafic ESP uniquement pour les tunnels VPN établis, abandonnant le trafic non associé à un tunnel existant. Cette restriction s'applique aux ports ESP et UDP 500 et 4500.
- Si vous définissez un VPN de site à site sur un périphérique qui se trouve derrière un périphérique qui applique la PAT dynamique, de sorte que les ports UDP 500 et 4500 ne soient pas ceux réellement utilisés, vous devez établir la connexion à partir du périphérique qui se trouve derrière la PAT. Le répondeur ne peut pas lancer l'association de sécurité (SA), car il ne connaît pas les bons numéros de port.
- Si vous modifiez la configuration NAT et que vous ne souhaitez pas attendre que les traductions existantes expirent avant d'utiliser la nouvelle configuration NAT, vous pouvez effacer le tableau de traduction à l'aide de la commande **clear xlate** dans la CLI du périphérique . Cependant, l'effacement du tableau de traduction déconnecte toutes les connexions actuelles qui utilisent des traductions.

  Si vous créez une nouvelle règle NAT qui doit s'appliquer à une connexion existante (comme un tunnel VPN), vous devez utiliser **clear conn** pour mettre fin à la connexion. Ensuite, la nouvelle tentative d'établissement de la connexion devrait correspondre à la règle NAT, et la traduction d'adresses devrait s'appliquer correctement.

Remarque Si vous supprimez une règle NAT ou PAT dynamique, puis ajoutez une nouvelle règle avec des adresses mappées qui chevauchent les adresses de la règle supprimée, la nouvelle règle ne sera pas utilisée tant que toutes les connexions associées à la règle supprimée n'auront pas expiré ou n'auront pas été effacées à l'aide de utilisez les commandes **clear xlate** ou **clear conn**. Cette mesure de protection garantit que la même adresse n'est pas attribuée à plusieurs hôtes.

- Vous ne pouvez pas utiliser un groupe d'objets avec des adresses IPv4 et IPv6 ; le groupe d'objets ne doit comprendre qu'un seul type d'adresse.
- Un objet réseau utilisé dans la NAT ne peut pas inclure plus de 131 838 adresses IP, explicitement ou implicitement dans une plage d'adresses ou un sous-réseau. Fractionnez l'espace d'adresse en plages plus petites et écrivez des règles distinctes pour les objets plus petits.
- (NAT manuelle seulement.) Lorsque vous utilisez **any** (n'importe laquelle) comme adresse source dans une règle NAT, la définition du trafic « tout » (IPv4 ou IPv6) dépend de la règle. Avant que Appareil FTD effectue la NAT sur un paquet, le paquet doit être IPv6-vers-IPv6 ou IPv4-vers-IPv4; avec cette condition préalable, Appareil FTD peut déterminer la valeur de **any** dans une règle NAT. Par exemple, si vous configurez une règle « any » pour un serveur IPv6, et que ce serveur a été mappé à partir d'une adresse IPv4, « **any** » signifie « tout trafic IPv6 ». Si vous configurez une règle de « any » à « any » et que vous mappez la source à l'adresse IPv4 de l'interface, « **any** » signifie « tout trafic IPv4 », car l'adresse d'interface mappée signifie que la destination est également IPv4.
- Vous pouvez utiliser le même objet ou groupe mappé dans plusieurs règles NAT.
- L'ensemble d'adresses IP mappées ne peut pas inclure :
  - L'adresse IP de l'interface mappée. Si vous spécifiez l'interface « any » pour la règle, toutes les adresses IP d'interface sont non autorisées. Pour l'interface PAT (mode routage uniquement), spécifiez le nom de l'interface au lieu de son adresse.
  - L'adresse IP de l'interface de basculement
  - (NAT dynamique.) L'adresse IP de l'interface de secours lorsque le VPN est activé.
- Évitez d'utiliser des adresses qui se chevauchent dans les politiques NAT statiques et dynamiques. Par exemple, avec des adresses qui se chevauchent, une connexion PPTP peut ne pas s'établir si la connexion secondaire pour PPTP atteint le xlate statique au lieu de dynamique.
- Vous ne pouvez pas utiliser des adresses qui se chevauchent dans l'adresse source d'une règle NAT et d'un ensemble d'adresses VPN d'accès à distance.
- Si vous spécifiez une interface de destination dans une règle, cette interface est utilisée comme interface de sortie plutôt que de rechercher la voie de routage dans la table de routage. Cependant, pour la NAT d'identité, vous avez la possibilité d'utiliser à la place une recherche de route.
- La NAT s'applique uniquement au trafic de transit. Le trafic généré par le système n'est pas soumis à la NAT.
- N'utilisez pas de combinaisons de lettres majuscules ou minuscules avant de nommer un objet réseau ou un ensemble TAP.

- Vous ne pouvez pas utiliser la NAT sur la charge utile interne des registres PIM (Protocol Independent Multicast).
- (NAT manuelle) lors de la rédaction de règles NAT pour une configuration d'interface ISP double (interfaces principale et de secours utilisant les contrats de niveau de service dans la configuration de routage), ne spécifiez pas de critères de destination dans la règle. Assurez-vous que la règle de l'interface principale précède la règle de l'interface de secours. Cela permet au périphérique de choisir la bonne interface de destination NAT en fonction de l'état de routage actuel lorsque le fournisseur de services Internet principal n'est pas disponible. Si vous spécifiez des objets de destination, la règle NAT sélectionnera toujours l'interface principale pour les règles autrement en double.
- Si vous obtenez la raison d'abandon ASP nat-no-xlate-to-pat- Pool pour le trafic qui ne devrait pas correspondre aux règles NAT définies pour l'interface, configurez les règles NAT d'identité pour le trafic affecté afin que le trafic puisse être non traduit.
- Si vous configurez la NAT pour les points terminaux d'un tunnel GRE, vous devez désactiver le maintien de l'activité sur les points terminaux, sinon le tunnel ne pourra pas être établi. Les points terminaux envoient des paquets keepalives aux adresses d'origine.
- DHCP et BOOTP partagent les ports UDP/67-68. Comme BOOTP est obsolète, l'écriture de règles NAT pour le port bootps peut entraîner des problèmes d'allocation de port lors de l'exécution de DHCP. Envisagez d'utiliser le relais DHCP plutôt pour transmettre les demandes DHCP entre les segments de réseau.
- Dans de rares cas, le trafic de retour (serveur à client) avec une traduction existante (xlate) peut être enregistré comme un nouveau flux dans les événements de connexion. Cela peut se produire lorsque le client a déjà mis fin à la connexion et que le serveur envoie un autre paquet qui atteint le périphérique pendant le court intervalle entre la fermeture de la connexion et le retrait de xlate, souvent en raison du comportement de l'application ou du nettoyage de la pile TCP. Comme le périphérique supprime le xlate uniquement après avoir supprimé la connexion, un paquet de serveur peut arriver pendant que le xlate existe toujours. Si aucune entrée de connexion valide n'est trouvée, le périphérique consigne un événement de connexion distinct en fonction de la règle de stratégie de contrôle d'accès correspondante.

Configurer la traduction d'adresses réseau (NAT)

La traduction d'adresses réseau peut être très complexe. Nous vous recommandons de garder vos règles aussi simples que possible pour éviter les problèmes de traduction et les situations de dépannage difficiles. Une planification rigoureuse avant de mettre en œuvre la NAT est essentielle. La procédure suivante fournit l'approche de base.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Décidez du type de règles dont vous avez besoin.

Vous pouvez créer des règles NAT dynamique, PAT dynamique, NAT statique et NAT d'identité. Pour un aperçu, consultez Types de NAT, à la page 566.

Étape 3 Décidez quelles règles doivent être mises en œuvre en tant que NAT manuelle ou automatique.

Pour une comparaison de ces deux options d'implémentation, consultez NAT automatique et NAT manuelle, à la page 568.

Étape 4 Créez les règles, comme expliqué dans les sections suivantes.

- Traduction d'adresses réseau dynamique, à la page 579
- PAT dynamique, à la page 584
- NAT statique, à la page 589
- NAT d'identité, à la page 598

Étape 5 Gérer la politique et les règles NAT

Vous pouvez effectuer ce qui suit pour gérer la politique et ses règles.

- Pour modifier une règle, cliquez sur l'icône de modification ( ) de la règle.
- Pour supprimer une règle, cliquez sur l'icône de suppression ( ) de la règle.

Traduction d'adresses réseau dynamique

Les rubriques suivantes expliquent la NAT dynamique et comment la configurer.

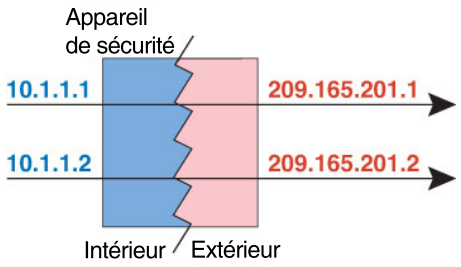
À propos de la NAT dynamique

La NAT dynamique traduit un groupe d'adresses réelles en un ensemble d'adresses mappées qui sont routables sur le réseau de destination. L'ensemble mappé comprend généralement moins d'adresses que le groupe réel. Lorsqu'un hôte que vous souhaitez traduire accède au réseau de destination, la NAT attribue à l'hôte une adresse IP de l'ensemble mappé. La traduction est créée uniquement lorsque l'hôte réel lance la connexion. La traduction n'est en place que pour la durée de la connexion et un utilisateur donné ne conserve pas la même adresse IP après l'expiration de la traduction. Par conséquent, les utilisateurs du réseau de destination ne peuvent pas établir de connexion fiable avec un hôte qui utilise la NAT dynamique, même si la connexion est autorisée par une règle d'accès.

Remarque Pour la durée de la traduction, un hôte distant peut établir une connexion avec l'hôte traduit si une règle d'accès le permet. Comme l'adresse est imprévisible, une connexion à l'hôte est peu probable. Cependant, dans ce cas, vous pouvez vous fier à la sécurité de la règle d'accès. Une connexion réussie à partir d'un hôte distant peut réinitialiser le minuteur d'inactivité de la connexion.

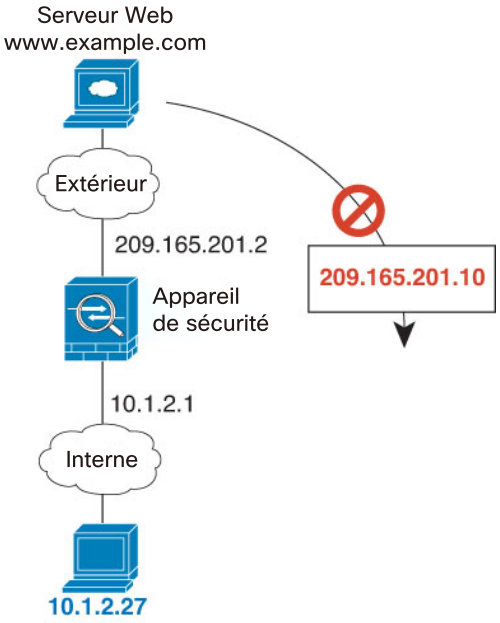
La figure suivante montre un scénario de NAT dynamique typique. Seuls les hôtes réels peuvent créer une session NAT, et le trafic qui répond est autorisé à revenir.

Illustration 11 : Traduction d'adresses réseau dynamique



La figure suivante montre un hôte distant tentant d'établir une connexion à une adresse mappée. Cette adresse ne figure pas dans la table de traduction actuellement; par conséquent, le paquet est abandonné.

Illustration 12 : L'hôte distant tente d'établir une connexion à une adresse mappée



Désavantages et avantages de la NAT dynamique

La NAT dynamique présente les désavantages suivants :

- Si l'ensemble mappé comporte moins d'adresses que le groupe réel, vous risquez de manquer d'adresses si le trafic est supérieur aux attentes.

  Utilisez PAT ou une méthode de secours PAT si cet événement se produit souvent, car PAT fournit plus de 64 000 traductions utilisant les ports d'une seule adresse.

- Vous devez utiliser un grand nombre d'adresses routables dans l'ensemble mappé, et les adresses routables peuvent ne pas être disponibles en grande quantité.

L'avantage de la NAT dynamique est que certains protocoles ne peuvent pas utiliser la PAT. La PAT ne fonctionne pas avec les éléments suivants :

- Les protocoles IP qui n'ont pas de port à surcharger, comme GRE version 0.

- Certaines applications multimédias qui ont un flux de données sur un port et le chemin de contrôle sur un autre port, et qui ne sont pas conformes aux normes ouvertes.

Configurer la NAT automatique dynamique

Utilisez les règles de NAT automatique dynamique pour traduire des adresses en différentes adresses IP qui sont routables sur le réseau de destination.

Avant de commencer

Sélectionnez **Objects** (Objets) et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Original Address (**Adresse d'origine) : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Adresse source traduite** : il peut s'agir d'un objet ou d'un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For** (Créer une règle pour) : sélectionnez **Auto NAT** (NAT automatique).
- **Type** : sélectionnez **Dynamic** (Dynamique).

Étape 4 Configurez les options de paquets de traduction suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.
- **Original Address** (Adresse d'origine) : l'objet réseau qui contient les adresses que vous traduisez.
- **Translated Address** (Adresse traduite) : l'objet réseau ou le groupe qui contient les adresses mappées.

Étape 5 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS correspondant à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle,

l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour obtenir plus de renseignements, consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT, à la page 642.

- **Passage à l'interface PAT (Interface de destination)** : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts.

Étape 6 Cliquez sur **OK**.

Configurer la NAT manuelle dynamique

Utilisez des règles de NAT manuelles dynamiques lorsque la NAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. La NAT dynamique traduit les adresses en différentes adresses IP qui sont routables sur le réseau de destination.

Avant de commencer

Sélectionnez **Objects** (Objets) et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Adresse source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Adresse source traduite** : il peut s'agir d'un objet ou d'un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.

Vous pouvez également créer des objets réseau pour la **destination d'origine** et la **destination traduite** si vous configurez une traduction statique pour ces adresses dans la règle.

Pour la NAT dynamique, vous pouvez également effectuer une traduction de port sur la destination. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour le port de **destination d'origine** et le **port de destination traduit**. Si vous spécifiez le port source, il sera ignoré.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

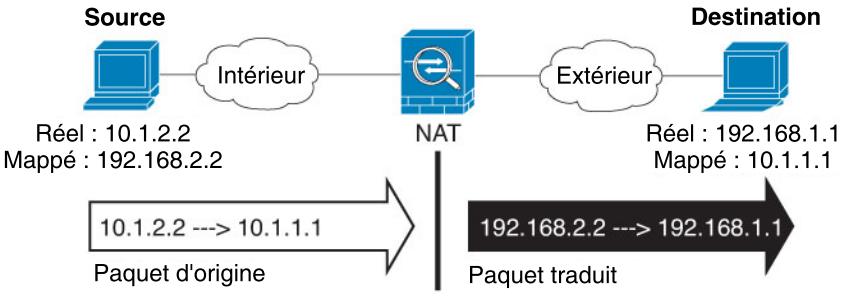
- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For**(Créer une règle pour) : sélectionnez **Manual NAT (NAT**manuelle).
- **Rule Placement** (Emplacement des règles) :Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous de la règle de votre choix.
- **Type** : sélectionnez **Dynamic** (Dynamique). Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.

Étape 4 Configurez les options d'interface suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



- **Original Source Address** (adresse de la source d'origine) : L'objet ou le groupe réseau qui contient les adresses que vous traduisez.
- **Original Destination Address** (adresse de la destination d'origine) (Facultatif) L'objet réseau qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Interface** pour baser la destination d'origine sur l'interface source (qui ne peut pas être réglée sur « Any »). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

Étape 6 Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Translated Source Address** (Adresse source traduite) : l'objet réseau ou le groupe qui contient les adresses mappées.

- **Translated Destination Address** (adresse de destination traduite) : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour l'**Original Destination Address (Destination d'origine**, vous pouvez configurer l'Identity NAT (NAT d'identité) en sélectionnant le même objet.

Étape 7 (Facultatif) Identifiez les ports de service de destination pour la traduction de service : **Original Destination Port** (port de la destination d'origine), **Translated Destination Port (port de la destination traduite)**.

Étant donné que la NAT dynamique ne prend pas en charge la traduction de port, laissez les champs **Original Source Port** (port de la source d'origine) et **Translated Source Port** (port de la source traduite) vides. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

Étape 8 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS correspondant à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour obtenir plus de renseignements, consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT, à la page 642.
- **Passage à l'interface PAT (Interface de destination)** : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts.

Étape 9 Cliquez sur **OK**.

PAT dynamique

Les rubriques suivantes décrivent la PAT dynamique.

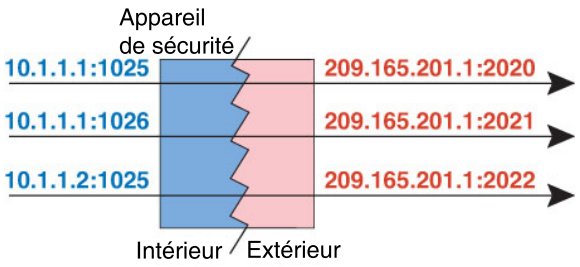
À propos de la PAT dynamique

La PAT dynamique traduit plusieurs adresses réelles en une seule adresse IP mappée en convertissant l'adresse réelle et le port source en adresse mappée et en un port unique.

Chaque connexion nécessite une session de traduction distincte, car le port source diffère pour chaque connexion. Par exemple, 10.1.1.1:1025 nécessite une traduction distincte de 10.1.1.1:1026.

La figure suivante montre un scénario PAT dynamique typique. Seuls les hôtes réels peuvent créer une session NAT, et le trafic qui répond est autorisé à revenir. L'adresse mappée est la même pour chaque traduction, mais le port est attribué dynamiquement.

Illustration 13 : PAT dynamique



Pour la durée de la traduction, un hôte distant sur le réseau de destination peut établir une connexion avec l'hôte traduit si une règle d'accès le permet. Comme l'adresse du port (réelle et mappée) est imprévisible, une connexion à l'hôte est peu probable. Cependant, dans ce cas, vous pouvez vous fier à la sécurité de la règle d'accès.

Après l'expiration de la connexion, la traduction de port expire également.

Remarque Nous vous recommandons d'utiliser différents ensembles de PAT pour chaque interface. Si vous utilisez le même ensemble pour plusieurs interfaces, en particulier si vous l'utilisez pour l'interface « n'importe quelle », l'ensemble peut être rapidement épuisé, et aucun port n'est disponible pour les nouvelles traductions.

Avantages et inconvénients de la PAT dynamique

La PAT dynamique vous permet d'utiliser une seule adresse mappée, préservant ainsi les adresses routables. Vous pouvez même utiliser l'adresse IP de l'interface Appareil FTD comme adresse PAT. Cependant, vous ne pouvez pas utiliser la PAT de l'interface pour les adresses IPv6 sur l'interface.

Vous ne pouvez pas utiliser la PAT dynamique pour IPv6 (NAT66) lors de la traduction entre les interfaces du même groupe de ponts. Cette restriction ne s'applique pas entre un membre d'un groupe de ponts et une interface routée standard.

La PAT dynamique ne fonctionne pas avec certaines applications multimédias dont le flux de données est différent de celui du chemin de contrôle. Pour obtenir plus de renseignements, consultez Prise en charge de la NAT pour les protocoles inspectés, à la page 574.

La PAT dynamique peut également créer un grand nombre de connexions semblant provenir d'une seule adresse IP, et les serveurs peuvent interpréter le trafic comme une attaque DoS.

Configurer la PAT automatique dynamique

Utilisez les règles PAT automatiques dynamiques pour traduire les adresses en combinaisons adresse IP/port uniques, plutôt qu'en plusieurs adresses IP uniquement. Vous pouvez traduire en une adresse unique, soit l'adresse de l'interface de destination, soit une autre adresse.

Avant de commencer

Sélectionnez **Objects** (Objets) et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Original Address (**Adresse d'origine) : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.

- **Translated Address** (Adresse traduite) : vous avez les options suivantes pour spécifier l'adresse PAT :
  - **Destination Interface** (Interface de destination) : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
  - **Adresse PAT unique** : crée un objet réseau contenant un seul hôte.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For** (Créer une règle pour) : sélectionnez **Auto NAT** (NAT automatique).
- **Type** : sélectionnez **Dynamic** (Dynamique).

Étape 4 Configurez les options de paquets de traduction suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.
- **Original Address** (Adresse d'origine) : l'objet réseau qui contient les adresses que vous traduisez.
- **Translated Address** (Adresse traduite) : l'une des adresses suivantes :
  - (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface**. Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
  - Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin.

Étape 5 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Transition vers l'interface PAT** (interface de destination) : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. vous ne pouvez pas sélectionner cette option si vous avez déjà configuré l'interface PAT comme adresse traduite. Vous ne pouvez pas utiliser cette option avec les réseaux IPv6.

Étape 6 Cliquez sur **OK**.

Configurer la PAT manuelle dynamique

Utilisez des règles PAT manuelles dynamiques lorsque la PAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. La PAT dynamique traduit les adresses en combinaisons adresse IP/port uniques, plutôt qu'en plusieurs adresses IP uniquement. Vous pouvez traduire en une adresse unique, soit l'adresse de l'interface de destination, soit une autre adresse.

Avant de commencer

Sélectionnez **Objects** (Objets) et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Adresse source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Adresse source traduite** : vous avez les choix suivants pour spécifier l'adresse PAT :
  - **Destination Interface** (Interface de destination) : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
  - **Adresse PAT unique** : crée un objet réseau contenant un seul hôte.

Vous pouvez également créer des objets réseau pour la **destination d'origine** et la **destination traduite** si vous configurez une traduction statique pour ces adresses dans la règle.

Pour la PAT dynamique, vous pouvez également effectuer une traduction de port sur la destination. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour le port de **destination d'origine** et le **port de destination traduit**. Si vous spécifiez le port source, il sera ignoré.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

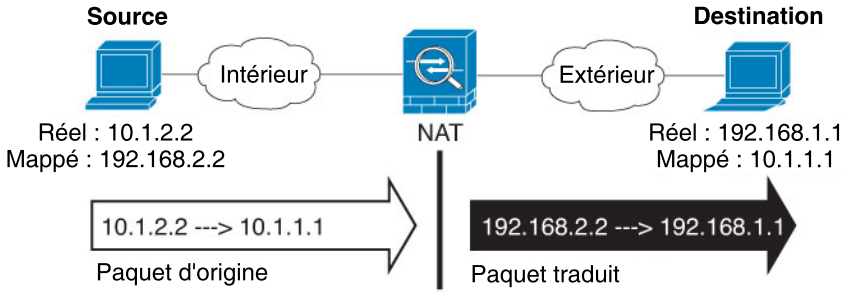
- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For**(Créer une règle pour) : sélectionnez **Manual NAT (NAT**manuelle).
- **Rule Placement** (Emplacement des règles) :Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous de la règle de votre choix.
- **Type** : sélectionnez **Dynamic** (Dynamique). Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.

Étape 4 Configurez les options d'interface suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



- **Original Source Address** (adresse de la source d'origine) : L'objet ou le groupe réseau qui contient les adresses que vous traduisez.
- **Original Destination Address** (adresse de la destination d'origine) (Facultatif) L'objet réseau qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Interface** pour baser la destination d'origine sur l'interface source (qui ne peut pas être réglée sur « Any »). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

Étape 6 Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Translated Source Address** (Source traduite) : l'une des suivantes :
  - (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface**. Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
  - Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin.
- **Translated Destination Address** (adresse de destination traduite) : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

Étape 7 (Facultatif) Identifiez les ports de service de destination pour la traduction de service : **Original Destination Port** (port de la destination d'origine), **Translated Destination Port (port de la destination traduite)**.

Étant donné que la NAT dynamique ne prend pas en charge la traduction de port, laissez les champs **Original Source Port** (port de la source d'origine) et **Translated Source Port** (port de la source traduite) vides. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

Étape 8 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Transition vers l'interface PAT** (interface de destination) : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. vous ne pouvez pas sélectionner cette option si vous avez déjà configuré l'interface PAT comme adresse traduite. Vous ne pouvez pas utiliser cette option avec les réseaux IPv6.

Étape 9 Cliquez sur **OK**.

NAT statique

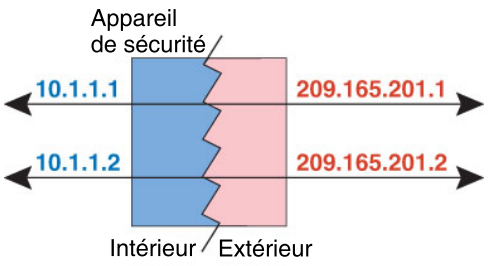
Les rubriques suivantes expliquent la NAT statique et comment la mettre en œuvre.

À propos de la NAT statique

La NAT statique crée une traduction fixe d'une adresse réelle en adresse mappée. Comme l'adresse mappée est la même pour chaque connexion consécutive, la NAT statique permet l'établissement d'une connexion bidirectionnelle, à la fois vers et à partir de l'hôte (si une règle d'accès existe qui le permet). Avec la NAT et la PAT dynamiques, en revanche, chaque hôte utilise une adresse ou un port différent pour chaque traduction ultérieure, de sorte que le lancement bidirectionnel n'est pas pris en charge.

La figure suivante montre un scénario de NAT statique typique. La traduction est toujours active, de sorte que les hôtes réels et distants peuvent initier des connexions.

Illustration 14 : NAT statique



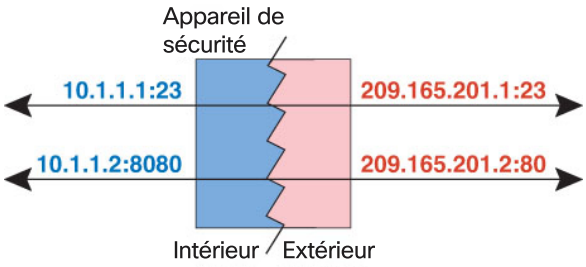
NAT statique avec traduction de port

La NAT statique avec traduction de port vous permet de spécifier un protocole et un port réels et mappés.

Lorsque vous spécifiez le port avec une NAT statique, vous pouvez choisir de mapper le port et/ou l'adresse IP à la même valeur ou à une valeur différente.

La figure suivante présente un scénario typique de NAT statique avec traduction de port, représentant à la fois un port mappé sur lui-même et un port mappé à une valeur différente. l'adresse IP est mappée sur une valeur différente dans les deux cas. La traduction est toujours active, donc les hôtes traduits et distants peuvent initier des connexions.

Illustration 15 : NAT statique typique avec scénario de traduction de port



Les règles statiques de NAT avec traduction de port limitent l'accès à l'adresse IP de destination pour le port spécifié uniquement. Si vous essayez d'accéder à l'adresse IP de destination sur un port différent non couvert par une règle NAT, la connexion est bloquée. De plus, pour NAT manuelle, le trafic qui ne correspond pas à l'adresse IP source de la règle NAT sera abandonné s'il correspond à l'adresse IP de destination, quel que soit le port de destination. Par conséquent, vous devez ajouter des règles supplémentaires pour tout autre trafic autorisé vers l'adresse IP de destination. Par exemple, vous pouvez configurer une règle NAT statique pour l'adresse IP, sans spécification de port, et la placer après la règle de traduction de port.

Remarque Pour les applications qui nécessitent une inspection d'application pour les canaux secondaires (par exemple, FTP et VoIP), la NAT traduit automatiquement les ports secondaires.

Voici quelques autres utilisations de la NAT statique avec traduction de port.

NAT statique avec traduction de port d'identité

Vous pouvez simplifier l'accès externe aux ressources internes. Par exemple, si vous avez trois serveurs distincts qui fournissent des services sur des ports différents (comme FTP, HTTP et SMTP), vous pouvez donner aux utilisateurs externes une seule adresse IP pour accéder à ces services. Vous pouvez ensuite configurer la NAT statique avec traduction de port d'identité pour mapper l'adresse IP externe unique avec les adresses IP correctes des serveurs réels en fonction du port auquel ils tentent d'accéder. Vous n'avez pas besoin de modifier le port, car les serveurs utilisent des ports standard (21, 80 et 25, respectivement).

NAT statique avec traduction de port pour les ports non standard

Vous pouvez également utiliser la NAT statique avec traduction de port pour traduire un port bien connu en un port non standard ou inversement. Par exemple, si les serveurs Web internes utilisent le port 8080, vous pouvez autoriser les utilisateurs externes à se connecter au port 80, puis annuler la traduction sur le port d'origine 8080. De même, pour fournir une sécurité supplémentaire, vous pouvez demander aux utilisateurs Web de se connecter au port non standard 6785, puis annuler la traduction sur le port 80.

NAT d'interface statique avec traduction de port

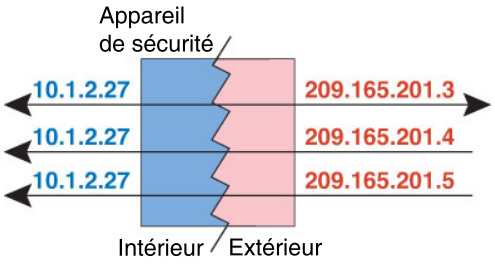
Vous pouvez configurer la NAT statique pour mapper une adresse réelle avec une combinaison adresse d'interface/port. Par exemple, si vous souhaitez rediriger l'accès Telnet pour l'interface externe du périphérique vers un hôte interne, vous pouvez mapper l'adresse IP/le port 23 de l'hôte interne avec l'adresse/le port 23 de l'interface externe.

NAT statique un vers plusieurs

En règle générale, vous configurez la NAT statique avec un mappage un à un. Cependant, dans certains cas, vous souhaiterez peut-être configurer une seule adresse réelle avec plusieurs adresses mappées (une vers plusieurs). Lorsque vous configurez la NAT statique un-vers-plusieurs, lorsque l'hôte réel lance le trafic, il utilise toujours la première adresse mappée. Cependant, pour le trafic initié vers l'hôte, vous pouvez initier le trafic vers n'importe laquelle des adresses mappées, et elles ne seront pas traduites vers l'adresse unique réelle.

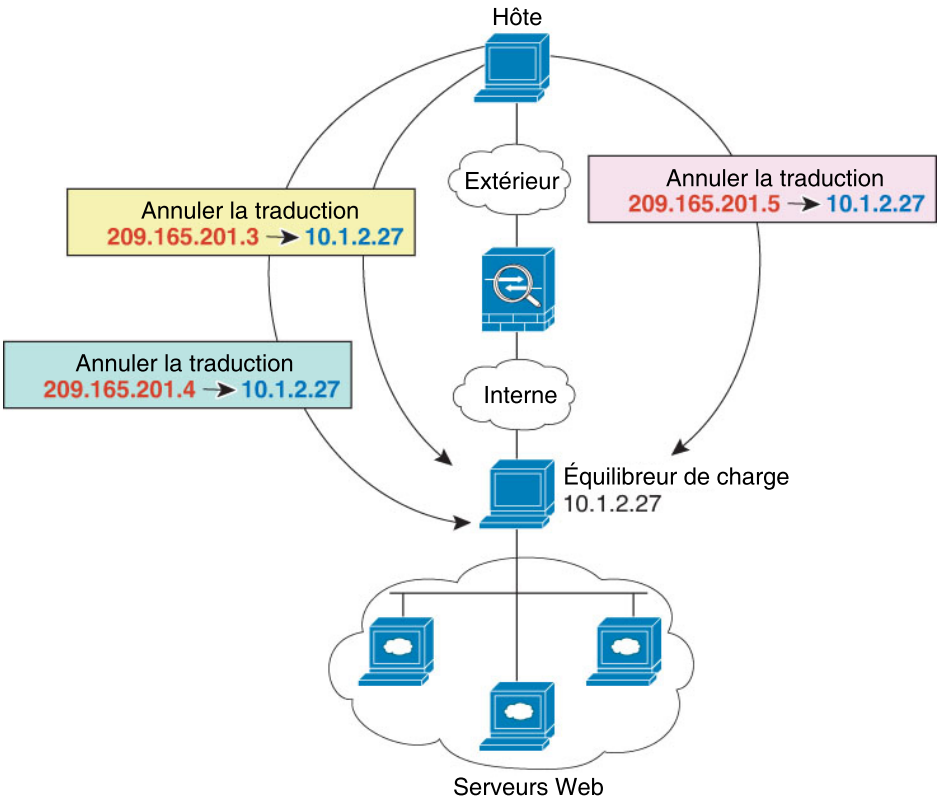
La figure suivante montre un scénario de NAT statique un-vers-plusieurs typique. Comme le lancement par l'hôte réel utilise toujours la première adresse mappée, la traduction IP de l'hôte réel/premier IP mappée est techniquement la seule traduction bidirectionnelle.

Illustration 16 : NAT statique un vers plusieurs



Par exemple, vous avez un équilibreur de charge en 10.1.2.27. Selon l'URL demandée, il redirige le trafic vers le bon serveur Web.

Illustration 17 : Exemple de NAT statique un vers plusieurs



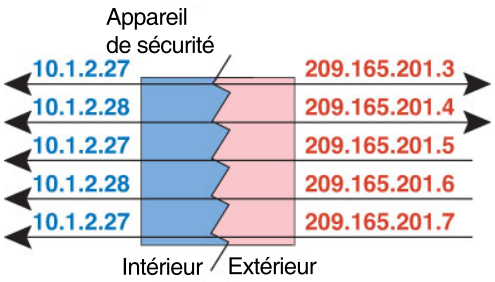
Autres scénarios de mappage (non recommandés)

La NAT a la flexibilité d'autoriser tout type de scénario de mappage statique : un à un, un à plusieurs, mais aussi les mappages de quelques-uns à plusieurs, de plusieurs à plusieurs et de plusieurs à un. Nous vous recommandons d'utiliser uniquement des mappages un à un ou un à plusieurs. Ces autres options de mappage peuvent avoir des conséquences imprévues.

D'un point de vue fonctionnel, les valeurs « peu à plusieurs » et « un à plusieurs » sont identiques. Mais comme la configuration est plus complexe et que les mappages ne sont peut-être pas évidents au premier abord, nous vous recommandons de créer une configuration un-vers-plusieurs pour chaque adresse réelle qui l'exige. Par exemple, pour un scénario de plusieurs vers plusieurs, les quelques adresses réelles sont mappées aux nombreuses adresses mappées dans l'ordre (A à 1, B à 2, C à 3). Lorsque toutes les adresses réelles sont mappées, l'adresse mappée suivante est mappée à la première adresse réelle, et ainsi de suite jusqu'à ce que toutes les adresses mappées soient mappées (A à 4, B à 5, C à 6). Il en résulte plusieurs adresses mappées pour chaque adresse réelle. Tout comme dans une configuration un-vers-plusieurs, seuls les premiers mappages sont bidirectionnels; les mappages suivants permettent d'amorcer le trafic *vers* l'hôte réel, mais tout le trafic en *provenance de* l'hôte réel utilise uniquement la première adresse mappée pour la source.

La figure suivante montre un scénario typique de NAT statique quelques-uns-plusieurs.

Illustration 18 : NAT statique quelques-uns vers plusieurs

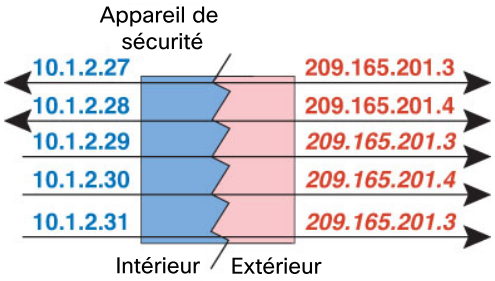


Pour une configuration plusieurs vers quelques ou plusieurs vers un, où vous avez plus d'adresses réelles que d'adresses mappées, vous manquez d'adresses mappées avant de manquer d'adresses réelles. Seuls les mappages entre les adresses IP réelles les plus basses et le groupement mappé entraînent un lancement bidirectionnel. Les adresses réelles supérieures restantes peuvent initier le trafic, mais le trafic ne peut pas être amorcé vers elles (le trafic de retour d'une connexion est redirigé vers la bonne adresse réelle en raison du quintuple unique (IP source, IP de destination, port source, port de destination,) pour la connexion).

Remarque La NAT plusieurs vers quelques ou plusieurs vers un n'est pas une PAT. Si deux hôtes réels utilisent le même numéro de port source et vont au même serveur externe et au même port de destination TCP, et que les deux hôtes sont traduits vers la même adresse IP, les deux connexions seront réinitialisées en raison d'un conflit d'adresse (le 5-uple n'est pas unique).

La figure suivante montre un scénario de NAT statique « plusieurs à quelques-uns » typique.

Illustration 19 : NAT statique plusieurs à quelques-uns



Au lieu d'utiliser une règle statique de cette façon, nous vous suggérons de créer une règle un-à-un pour le trafic qui nécessite un lancement bidirectionnel, puis de créer une règle dynamique pour le reste de vos adresses.

Configurer la NAT statique automatique

Utilisez les règles de NAT automatique statique pour traduire des adresses en différentes adresses IP qui sont routables sur le réseau de destination. Vous pouvez également effectuer une traduction de port avec la règle NAT statique.

Avant de commencer

Sélectionnez **Objects** (Objets) et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Original Address (**Adresse d'origine) : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Translated Address** (Adresse traduite) : vous avez les options suivantes pour spécifier l'adresse traduite :
  - **Destination Interface** (Interface de destination) : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau. Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
  - **Address** (Adresse) : crée un objet réseau ou un groupe contenant des hôtes, une plage, ou des sous-réseaux. Un groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For** (Créer une règle pour) : sélectionnez **Auto NAT** (NAT automatique).
- **Type** : sélectionnez **Statique**.

Étape 4 Configurez les options de paquets de traduction suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.
- **Original Address** (Adresse d'origine) : l'objet réseau qui contient les adresses que vous traduisez.
- **Translated Address** (Adresse traduite) : l'une des adresses suivantes :
  - Pour utiliser un groupe d'adresses défini, sélectionnez Address (adresse), puis l'objet ou le groupe de réseau qui contient les adresses mappées. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.
  - (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface** (Adresse IP de l'interface de destination). Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.Cela configure la NAT de l'interface

statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.

- (Facultatif) **Original Port (Port d'origine)**, **Translated Port (Port traduit)** : si vous devez traduire un port TCP ou UDP, sélectionnez le protocole dans Port d'origine et saisissez les numéros de port d'origine et traduit. Les objets doivent être pour le même protocole. Cliquez sur le lien **Create New Object** (Créer un nouvel objet) si les objets n'existent pas déjà. Par exemple, vous pouvez traduire TCP/80 en TCP/8080 au besoin.

Étape 5 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour obtenir plus de renseignements, consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT, à la page 642. Cette option n'est pas disponible si vous effectuez une traduction de port.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.

Étape 6 Cliquez sur **OK**.

Configurer la NAT manuelle statique

Utilisez des règles de NAT manuelle statique lorsque la NAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. La NAT statique traduit les adresses en différentes adresses IP qui sont routables sur le réseau de destination. Vous pouvez également effectuer une traduction de port avec la règle NAT statique.

Avant de commencer

Sélectionnez **Objects** (Objets) et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Adresse source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Translated Source Address** (Adresse source traduite : vous avez les options suivantes pour spécifier l'adresse traduite :

- **Destination Interface** (Interface de destination) : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau. Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
- **Address** (Adresse) : crée un objet réseau ou un groupe contenant des hôtes, une plage, ou des sous-réseaux. Un groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.

Vous pouvez également créer des objets réseau pour **Original Destination Address** (Adresse de destination d'origine et **Translated Destination Address** (Adresse de destination traduite) si vous configurez une traduction statique pour ces adresses dans la règle. Si vous souhaitez configurer la NAT de l'interface statique de destination avec traduction de port uniquement, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées de destination et préciser l'interface dans la règle.

Vous pouvez également effectuer une traduction de port sur la source, la destination ou les deux. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour les ports d'origine et les ports traduits.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

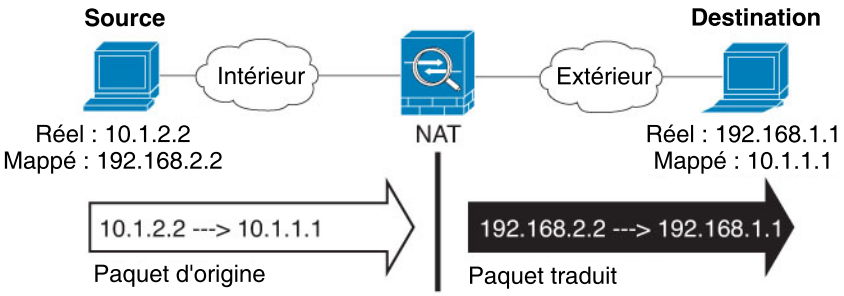
- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For**(Créer une règle pour) : sélectionnez **Manual NAT (NAT**manuelle).
- **Rule Placement** (Emplacement des règles) :Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous de la règle de votre choix.
- **Type** : sélectionnez **Statique**. Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.

Étape 4 Configurez les options d'interface suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



- **Original Source Address** (adresse de la source d'origine) : L'objet ou le groupe réseau qui contient les adresses que vous traduisez.
- **Original Destination Address** (adresse de la destination d'origine) (Facultatif) L'objet réseau qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Interface** pour baser la destination d'origine sur l'interface source (qui ne peut pas être réglée sur « Any »). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

Étape 6 Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Translated Source Address** (Source traduite) : l'une des suivantes :
  - Pour utiliser un groupe d'adresses défini, sélectionnez Address (adresse), puis l'objet ou le groupe de réseau qui contient les adresses mappées. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.
  - (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface**. Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
- **Translated Destination Address** (adresse de destination traduite) : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

Étape 7 (Facultatif) Déterminez les ports du service source ou de destination pour la traduction de service.

Si vous configurez une NAT statique avec traduction de port, vous pouvez traduire les ports pour la source, la destination ou les deux. Par exemple, vous pouvez traduire entre TCP/80 et TCP/8080.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

- **Port source d'origine**, **Port source traduit** : définit une traduction de port pour l'adresse source.
- **Port de destination d'origine**, **Port de destination traduit** : définit une traduction de port pour l'adresse de destination.

Étape 8 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour obtenir plus de renseignements, consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT, à la page 642. Cette option n'est pas disponible si vous effectuez une traduction de port.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.

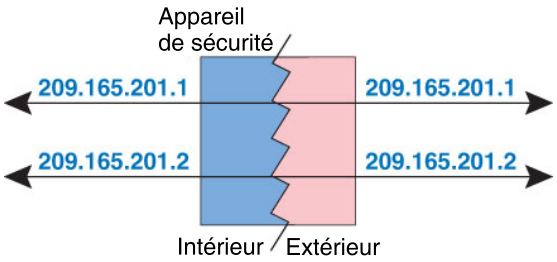
Étape 9 Cliquez sur **OK**.

NAT d'identité

Vous pouvez avoir une configuration NAT dans laquelle vous devez traduire une adresse IP vers elle-même. Par exemple, si vous créez une règle générale qui applique la NAT à tous les réseaux, mais que vous souhaitez exclure un réseau de la NAT, vous pouvez créer une règle NAT statique pour traduire une adresse vers elle-même.

La figure suivante montre un scénario de NAT d'identité typique.

Illustration 20 : NAT d'identité



Les rubriques suivantes expliquent comment configurer la NAT d'identité.

Configurer la NAT automatique d'identité

Utilisez les règles de NAT automatique d'identité statique pour empêcher la traduction d'une adresse. C'est-à-dire pour traduire l'adresse dans elle-même.

Avant de commencer

Sélectionnez **Objects** (Objets) et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Original Address (**Adresse d'origine) : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Source traduite** : objet ou groupe réseau ayant exactement le même contenu que l'objet source d'origine. Vous pouvez utiliser le même objet.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For** (Créer une règle pour) : sélectionnez **Auto NAT** (NAT automatique).
- **Type** : sélectionnez **Statique**.

Étape 4 Configurez les options de paquets de traduction suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.
- **Original Address** (Adresse d'origine) : l'objet réseau qui contient les adresses que vous traduisez.
- **Adresse traduite** : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

Ne configurez pas les options de **port d'origine** et de **port traduit** pour la NAT d'identité.

Étape 5 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : ne configurez pas cette option pour la NAT d'identité.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage,

car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.

- **Effectuer une consultation de route pour l'interface de destination**—Si vous sélectionnez les interfaces source et destination lorsque vous sélectionnez le même objet pour l'adresse source originale et traduite, vous pouvez choisir cette option pour veiller à ce que le système détermine l'interface de destination en fonction de la table de routage et pas de l'interface de destination configurée dans la règle NAT.

Étape 6 Cliquez sur **OK**.

Configurer la NAT manuelle d'identité

Utilisez les règles NAT manuelles d'identité statique lorsque la NAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. Utilisez les règles NAT d'identité statique pour empêcher la traduction d'une adresse. C'est-à-dire pour traduire l'adresse dans elle-même.

Avant de commencer

Sélectionnez **Objects** (Objets) et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Adresse source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Translated Source Address** (Adresse source traduite) : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

Vous pouvez également créer des objets réseau pour **Original Destination Address** (Adresse de destination d'origine et **Translated Destination Address** (Adresse de destination traduite) si vous configurez une traduction statique pour ces adresses dans la règle. Si vous souhaitez configurer la NAT de l'interface statique de destination avec traduction de port uniquement, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées de destination et préciser l'interface dans la règle.

Vous pouvez également effectuer une traduction de port sur la source, la destination ou les deux. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour les ports d'origine et les ports traduits. Vous pouvez utiliser le même objet pour la NAT d'identité.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

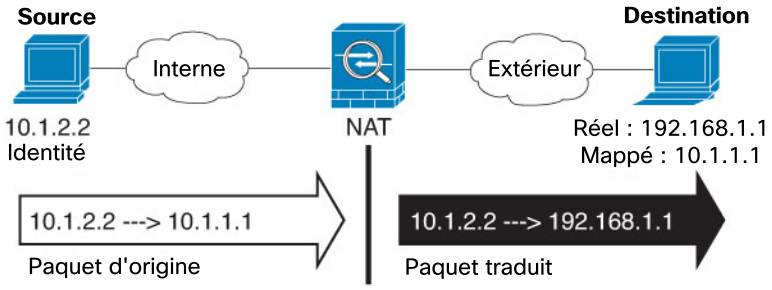
- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For**(Créer une règle pour) : sélectionnez **Manual NAT (NAT**manuelle).
- **Rule Placement** (Emplacement des règles) :Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous de la règle de votre choix.
- **Type** : sélectionnez **Statique**. Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.

Étape 4 Configurez les options d'interface suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Consultez la figure suivante pour un exemple de paquet d'origine par rapport au paquet traduit dans lequel vous effectuez une NAT d'identité sur l'hôte interne, mais traduit l'hôte externe.



- **Original SourceAddress** (adresse de la source d'origine) : l'objet ou le groupe réseau qui contient les adresses que vous traduisez.
- **Original DestinationAddress** (Adresse de la destination d'origine) (Facultatif) L'objet réseau qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Interface** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

Étape 6 Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Translated Source Address** (Adresse source traduite) : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

- **Translated Destination Address** (adresse de destination traduite) : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour l'**Original Destination Address (Destination d'origine**, vous pouvez configurer l'Identity NAT (NAT d'identité) en sélectionnant le même objet.

Étape 7 (Facultatif) Déterminez les ports du service source ou de destination pour la traduction de service.

Si vous configurez une NAT statique avec traduction de port, vous pouvez traduire les ports pour la source, la destination ou les deux. Par exemple, vous pouvez traduire entre TCP/80 et TCP/8080.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

- **Port source d'origine**, **Port source traduit** : définit une traduction de port pour l'adresse source.
- **Port de destination d'origine**, **Port de destination traduit** : définit une traduction de port pour l'adresse de destination.

Étape 8 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : ne configurez pas cette option pour la NAT d'identité.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.
- **Effectuer une consultation de route pour l'interface de destination** : Si vous sélectionnez les interfaces source et destination lorsque vous sélectionnez le même objet pour l'adresse source originale et traduite, vous pouvez choisir cette option pour veiller à ce que le système détermine l'interface de destination en fonction de la table de routage et pas de l'interface de destination configurée dans la règle NAT.

Étape 9 Cliquez sur **OK**.

Propriétés de la règle NAT pour Firewall Threat Defense

Utilisez les règles de traduction d'adresses réseau (NAT) pour traduire des adresses IP en d'autres adresses IP. Vous utilisez généralement des règles NAT pour convertir des adresses privées en adresses publiquement routables. La traduction peut se faire d'une adresse à une autre, ou vous pouvez utiliser la Port Address Translation (PAT) pour traduire plusieurs adresses vers une seule, en utilisant des numéros de port pour distinguer les adresses source.

Les règles NAT comprennent les propriétés de base suivantes. Les propriétés sont les mêmes pour les règles NAT automatique et manuelle, sauf mention contraire.

Titre

Entrez un nom pour la règle. Le nom ne peut pas contenir d'espaces.

Create Rule For (Créer une règle pour)

Que la règle de traduction soit **Auto NAT** (NAT automatique) ou **Manual NAT** (NAT manuelle). La NAT automatique est plus simple que la NAT manuelle, mais la NAT manuelle vous permet de créer des traductions distinctes pour une adresse source en fonction de l'adresse de destination.

État

Indique si vous souhaitez que la règle soit active ou désactivée.

Placement (NAT manuelle uniquement)

Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous de la règle de votre choix.

Type

Si la règle de traduction est **Dynamique** ou **Statique**. La traduction dynamique choisit automatiquement l'adresse mappée dans un ensemble d'adresses ou une combinaison adresse/port lors de la mise en œuvre de la PAT. Utilisez la traduction statique si vous souhaitez définir avec précision l'adresse ou le port mappé.

Les rubriques suivantes décrivent les propriétés restantes des règles NAT.

Propriétés de traduction de paquets pour la NAT automatique

Utilisez les options **Packet Translation** (Traduction de paquets) pour définir les adresses source et les adresses traduites mappées. Les propriétés suivantes s'appliquent uniquement à la NAT automatique.

Source Interface (Interface source), Destination Interface (Interface de destination)

(obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Original Address (Adresse d'origine) (toujours obligatoire)

L'objet réseau qui contient les adresses source que vous traduisez. Cela doit être un objet réseau (et non un groupe), et il peut s'agir d'un hôte, d'une plage, ou d'un sous-réseau.

Translated Address (Adresse traduite) (généralement requise)

Les adresses mappées, celles vers lesquelles vous effectuez la traduction. Ce que vous sélectionnez ici dépend du type de règle de traduction que vous définissez.

- **NAT dynamique** : objet ou groupe réseau qui contient les adresses mappées. Il peut s'agir d'un objet ou d'un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.
- **PAT dynamique** : l'un des éléments suivants :
  - (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface**. Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.

- Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin.

- **NAT statique** : l'une des options suivantes :
  - Pour utiliser un groupe d'adresses défini, sélectionnez l'objet ou le groupe de réseau qui contient les adresses mappées. L'objet ou le groupe peut contenir des hôtes, des plages ou des sous-réseaux. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.
  - (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface** (Adresse IP de l'interface de destination). Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.

- **NAT d'identité** : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

Port d'origine, Port traduit (NAT statique uniquement)

Si vous devez traduire un port TCP ou UDP, sélectionnez les objets de port qui définissent les ports d'origine et traduits. Les objets doivent être pour le même protocole. Par exemple, vous pouvez traduire TCP/80 en TCP/8080 au besoin.

Propriétés de traduction de paquets pour la NAT manuelle

Utilisez les options **Packet Translation** (Traduction de paquets) pour définir les adresses source et les adresses traduites mappées. Les propriétés suivantes s'appliquent uniquement à la NAT manuelle. Tous ces éléments sont facultatifs, sauf indication contraire.

Source Interface (Interface source), Destination Interface (Interface de destination)

(obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Original Source Address (Adresse source d'origine) (toujours obligatoire)

L'objet ou le groupe de réseaux qui contient les adresses que vous traduisez. Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez spécifier **Any** (Tout) dans la règle.

Translated Source Address (Adresse source traduite) (généralement requise)

Les adresses mappées, celles vers lesquelles vous effectuez la traduction. Ce que vous sélectionnez ici dépend du type de règle de traduction que vous définissez.

- **NAT dynamique** : objet ou groupe réseau qui contient les adresses mappées. Il peut s'agir d'un objet ou d'un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT

dynamique, puis les adresses IP de l'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.

- **PAT dynamique** : l'un des éléments suivants :
  - (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface** (Adresse IP de l'interface de destination). Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
  - Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin.
- **NAT statique** : l'une des options suivantes :
  - Pour utiliser un groupe d'adresses défini, sélectionnez l'objet ou le groupe de réseau qui contient les adresses mappées. L'objet ou le groupe peut contenir des hôtes, des plages ou des sous-réseaux. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.
  - (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface** (Adresse IP de l'interface de destination). Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
- **NAT d'identité** : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

Adresse de destination d'origine

L'objet réseau qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

Vous pouvez sélectionner **Interface** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

Adresse de destination traduite

L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

Port source d'origine, Port source traduit, Port de destination d'origine, Port de destination traduit

Les objets de port qui définissent les services de source et de destination pour les paquets d'origine et les paquets traduits. Vous pouvez traduire les ports ou sélectionner le même objet pour rendre la règle sensible au service sans traduire les ports. Gardez les règles suivantes à l'esprit lors de la configuration des services :

- (NAT ou PAT dynamique.) Vous ne pouvez pas effectuer de traduction sur le **port source d' origine** et le **port source traduit**. Vous ne pouvez effectuer la traduction que sur le port de destination.
- La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet pour les ports réels et mappés.

Propriétés NAT avancées

Lorsque vous configurez la NAT, vous pouvez configurer les propriétés qui fournissent des services spécialisés dans les options **avancées**. Toutes ces propriétés sont facultatives : ne les configurez que si vous avez besoin du service.

Traduire les réponses DNS correspondant à cette règle

Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour obtenir plus de renseignements, consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT, à la page 642. Cette option n'est pas disponible si vous effectuez une traduction de port dans une règle NAT statique.

Passage à l'interface PAT (Interface de destination) (NAT dynamique uniquement).

Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. Vous ne pouvez pas sélectionner cette option si vous avez déjà configuré l'interface PAT comme adresse traduite. Vous ne pouvez pas utiliser cette option avec les réseaux IPv6.

Ne pas mandater l'ARP sur l'Interface de destination(NAT statique uniquement).

Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.

Effectuer une consultation de route pour l'interface de destination (NAT d'identité statique uniquement. Mode routé uniquement.)

Si vous sélectionnez les interfaces source et destination lorsque vous sélectionnez le même objet pour l'adresse source originale et traduite, vous pouvez choisir cette option pour veiller à ce que le système détermine l'interface de destination en fonction de la table de routage et pas de l'interface de destination configurée dans la règle NAT.

Traduction de réseaux IPv6

Dans les cas où vous devez transférer du trafic entre des réseaux IPv6 uniquement et des réseaux IPv4 uniquement, vous devez utiliser la NAT pour convertir les types d'adresses. Même avec deux réseaux IPv6, vous souhaiterez peut-être masquer les adresses internes du réseau externe.

Vous pouvez utiliser les types de traduction suivants avec les réseaux IPv6 :

- NAT64, NAT46 : Traduit les paquets IPv6 en IPv4 et vice versa. Vous devez définir deux politiques, une pour la traduction d'IPv6 à IPv4 et une pour la traduction d'IPv4 à IPv6. Bien que vous puissiez accomplir cela à l'aide d'une seule règle NAT manuelle, si le serveur DNS se trouve sur le réseau externe, vous devrez probablement réécrire la réponse DNS. Comme vous ne pouvez pas activer la réécriture DNS sur une règle NAT manuelle lorsque vous spécifiez une destination, la création de deux règles auto NAT est la meilleure solution.



Remarque NAT46 prend uniquement en charge les mappages statiques.

- NAT66 : traduit les paquets IPv6 en une adresse IPv6 différente. Nous vous recommandons d'utiliser la NAT statique. Bien que vous puissiez utiliser la NAT ou la PAT dynamique, les adresses IPv6 sont si nombreuses que vous n'êtes pas obligé d'utiliser la NAT dynamique.



Remarque NAT64 et NAT 46 ne sont possibles que sur les interfaces routées standard. NAT66 est possible sur les interfaces routées et les membres du groupe de ponts.

NAT64/46 : traduction d'adresses IPv6 en IPv4

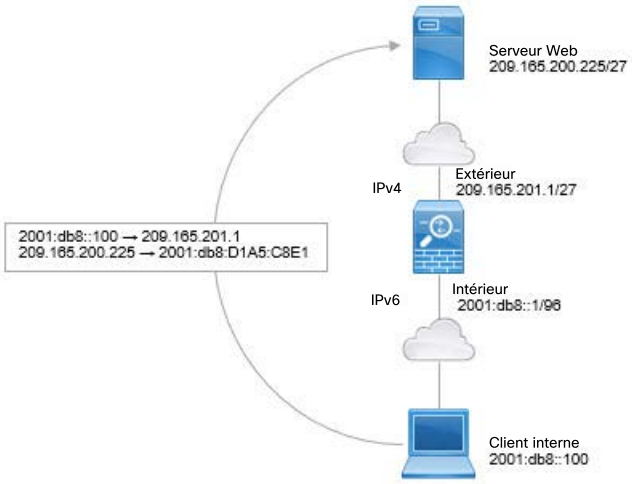
Lorsque le trafic passe d'un réseau IPv6 vers un réseau uniquement IPv4, vous devez convertir l'adresse IPv6 en IPv4 et renvoyer le trafic d'IPv4 à IPv6. Vous devez définir deux ensembles d'adresses, un ensemble d'adresses IPv4 pour lier les adresses IPv6 dans le réseau IPv4 et un ensemble d'adresses IPv6 pour lier les adresses IPv4 dans le réseau IPv6.

- L'ensemble d'adresses IPv4 pour la règle NAT64 est normalement de petite taille et peut généralement ne pas avoir assez d'adresses pour un mappage individuel avec les adresses client IPv6. La PAT dynamique pourrait plus facilement répondre au plus grand nombre possible d'adresses de clients IPv6 par rapport à la NAT dynamique ou statique.
- L'ensemble d'adresses IPv6 pour la règle NAT46 peut être égal ou supérieur au nombre d'adresses IPv4 à mapper. Cela permet de faire correspondre chaque adresse IPv4 à une adresse IPv6 différente. NAT46 prend uniquement en charge les mappages statiques, vous ne pouvez donc pas utiliser la PAT dynamique.

Vous devez définir deux politiques, une pour le réseau IPv6 source et une pour le réseau IPv4 de destination. Bien que vous puissiez accomplir cela à l'aide d'une seule règle NAT manuelle, si le serveur DNS se trouve sur le réseau externe, vous devrez probablement réécrire la réponse DNS. Comme vous ne pouvez pas activer la réécriture DNS sur une règle NAT manuelle lorsque vous spécifiez une destination, la création de deux règles auto NAT est la meilleure solution.

Exemple NAT64/46 : réseau IPv6 interne avec Internet IPv4 externe

Voici un exemple simple où vous avez un réseau interne IPv6 uniquement et que vous souhaitez convertir à IPv4 pour le trafic envoyé sur Internet. Cet exemple suppose que vous n'avez pas besoin de la traduction DNS, de sorte que vous pouvez effectuer les traductions NAT64 et NAT46 dans une seule règle NAT manuelle.



Dans cet exemple, vous allez traduire le réseau IPv6 interne en IPv4 à l'aide de l'interface dynamique PAT avec l'adresse IP de l'interface externe. Le trafic IPv4 externe est converti statiquement en adresses sur le réseau 2001:db8::/96, ce qui permet la transmission sur le réseau interne.

Procédure

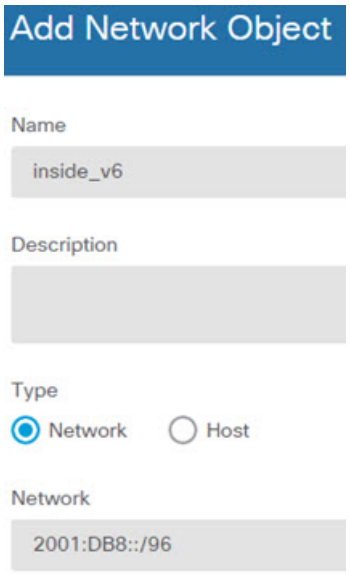
Étape 1 Créez un objet réseau pour le réseau IPv6 interne.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur **+**.

c) Définissez le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, inside_v6), sélectionnez **Network** (réseau), puis saisissez l'adresse réseau 2001:db8::/96.

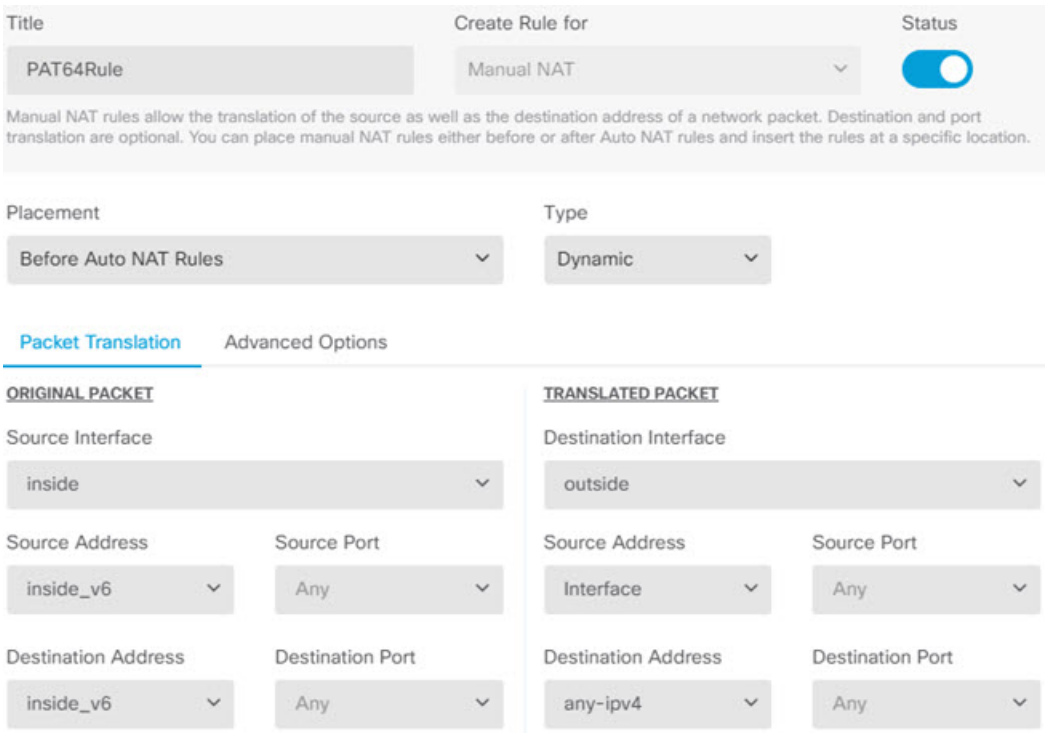


d) Cliquez sur **OK**.

Étape 2 Créez la règle NAT manuelle pour traduire le réseau IPv6 en IPv4 et inversement.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton **+**.
c) Configurez les propriétés suivantes :

- **Titre** = PAT64Rule (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = **Manual NAT** (NAT manuelle).
- **Placement** (emplacement) = **Before Auto NAT Rules** (avant les règles NAT automatiques)
- **Type** = **Dynamic** (dynamique).
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Original Packet Source Address** (adresse source de paquet d'origine) = objet réseau inside_v6.
- **Translated Packet Source Address (adresse source de paquet traduite)** = Interface. Cette option utilise l'adresse IPv4 de l'interface de destination comme adresse PAT.
- **Original Packet Destination Address** (adresse de destination de paquet d'origine) = objet réseau inside_v6.
- **Translated Packet Destination Address** (adresse de destination de paquet traduite) = objet réseau any-ipv4.

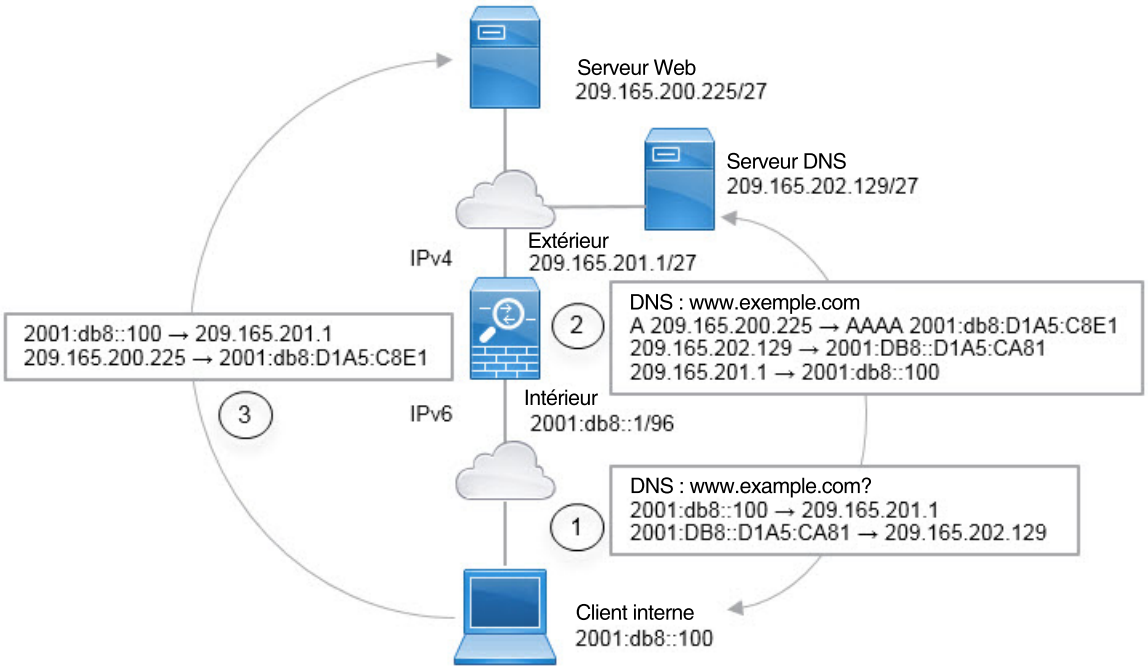


d) Cliquez sur **OK**.

Avec cette règle, tout trafic du sous-réseau 2001:db8::/96 sur l'interface interne à destination de l'interface externe reçoit une traduction PAT NAT64 utilisant l'adresse IPv4 de l'interface externe. Inversement, toute adresse IPv4 du réseau externe acheminée à l'interface interne est traduite en adresse sur le réseau 2001:db8::/96 à l'aide de la méthode de l'adresse IPv4 intégrée.

Exemple NAT64/46 : réseau interne IPv6 avec Internet IPv4 externe et traduction DNS

Voici un exemple typique dans lequel vous avez un réseau interne IPv6 uniquement, mais il existe certains services IPv4 uniquement sur Internet externe dont les utilisateurs internes ont besoin.



Dans cet exemple, vous allez traduire le réseau IPv6 interne en IPv4 à l'aide de l'interface dynamique PAT avec l'adresse IP de l'interface externe. Le trafic IPv4 externe est converti statiquement en adresses sur le réseau 2001:db8::/96, ce qui permet la transmission sur le réseau interne. Vous activez la réécriture DNS sur la règle NAT46, afin que les réponses du serveur DNS externe puissent être converties d'enregistrements A (IPv4) en enregistrements AAAA (IPv6) et les adresses converties d'IPv4 à IPv6.

Voici une séquence typique d'une requête Web où un client à l'adresse 2001:DB8::100 sur le réseau IPv6 interne tente d'ouvrir www.example.com.

1. L'ordinateur du client envoie une requête DNS au serveur DNS à l'adresse 2001:DB8::D1A5:CA81. Les règles NAT effectuent les traductions suivantes pour la source et la destination dans la requête DNS :
   - 2001:DB8::100 sur un port unique sur 209.165.201.1 (règle PAT de l'interface NAT64.)
   - 2001:DB8::D1A5:CA81 à 209.165.202.129 (la règle NAT46. D1A5 : CA81 est l'équivalent IPv6 de 209.165.202.129.)
2. Le serveur DNS répond par un enregistrement A, indiquant que www.example.com est au 209.165.200.225. La règle NAT46, avec la réécriture DNS activée, convertit l'enregistrement A en enregistrement AAAA équivalent au protocole IPv6, et traduit 209.165.200.225 en 2001:db8:D1A5:C8E1 dans l'enregistrement AAAA. De plus, les adresses de source et de destination dans la réponse DNS ne sont pas traduites :
   - 209.165.202.129 to 2001:DB8::D1A5:CA81
   - 209.165.201.1 to 2001:db8::100
3. Le client IPv6 a maintenant l'adresse IP du serveur Web et envoie une requête HTTP à www.example.com à l'adresse 2001:db8:D1A5:C8E1. (D1A5:C8E1 is the IPv6 equivalent of 209.165.200.225.) La source et la destination de la requête HTTP sont traduites :
   - 2001:DB8::100 sur un port unique sur 209.156.101.54 (règle PAT de l'interface NAT64).
   - 2001:db8:D1A5:C8E1 à 209.165.200.225 (la règle NAT46.)

La procédure suivante explique comment configurer cet exemple.

Procédure

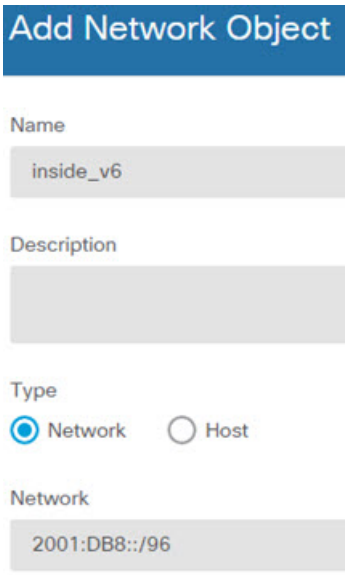
Étape 1 Créez les objets réseau qui définissent les réseaux IPv6 internes et externes IPv4.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.

c) Définissez le réseau IPv6 interne.

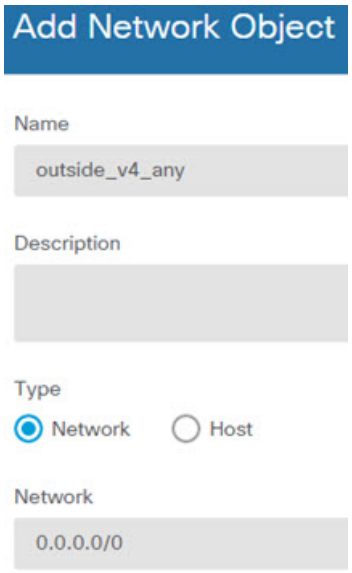
Nommez l'objet réseau (par exemple, inside_v6), sélectionnez **Network** (réseau), puis saisissez l'adresse réseau 2001:db8::/96.



d) Cliquez sur **OK**.

e) Cliquez sur + et définissez le réseau IPv4 externe.

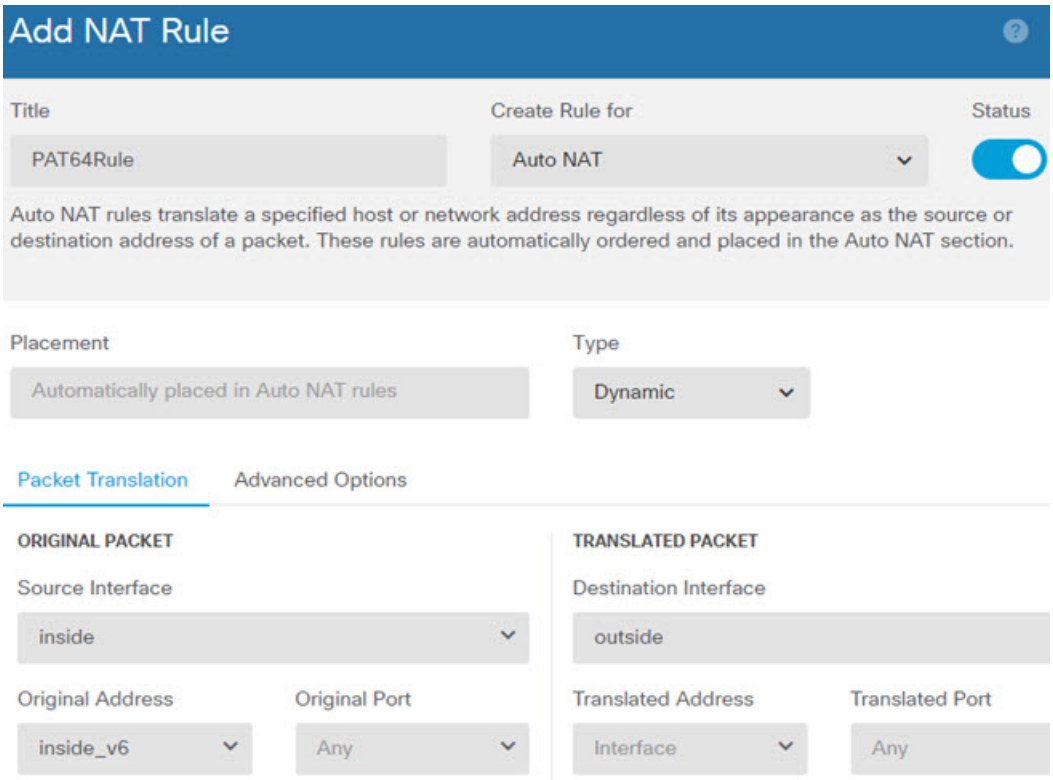
Nommez l'objet réseau (par exemple, outside_v4_any), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau 0.0.0.0/0.



Étape 2 Configurez la règle PAT dynamique NAT64 pour le réseau IPv6 interne.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton **+**.
c) Configurez les propriétés suivantes :

- **Titre** = PAT64Rule (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse originale** = inside_v6 network object.
- **Translated Address** (Adresse traduite) = **Interface**. Cette option utilise l'adresse IPv4 de l'interface de destination comme adresse PAT.



d) Cliquez sur **OK**.

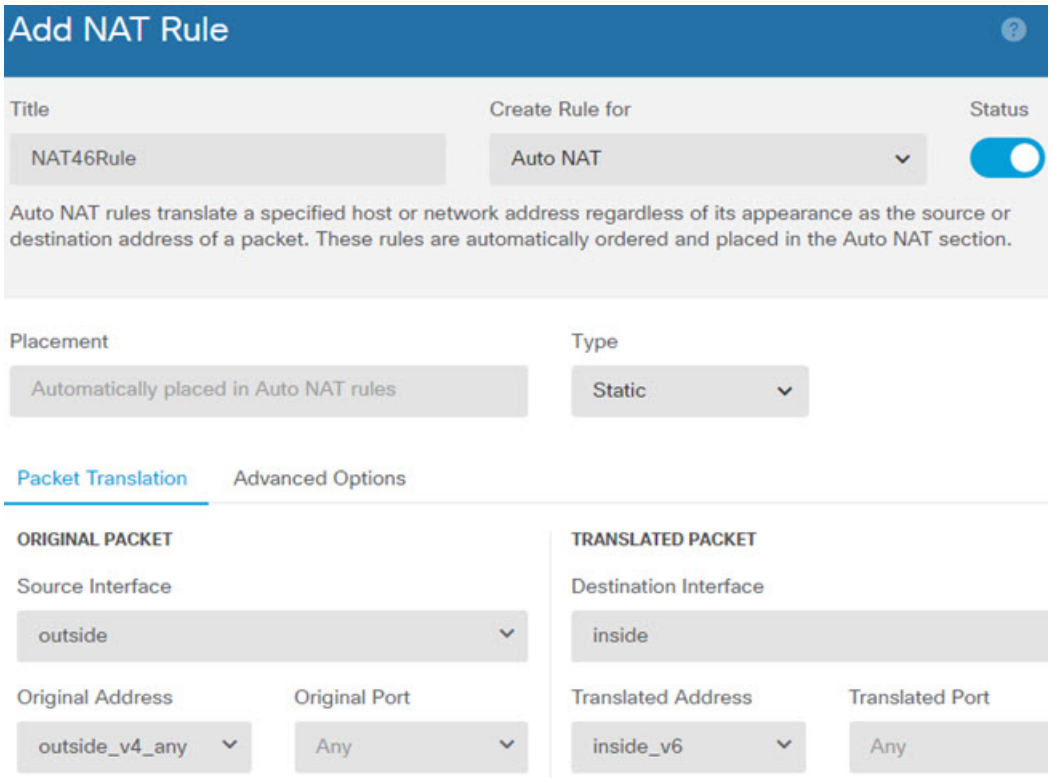
Avec cette règle, tout trafic du sous-réseau 2001:db8::/96 sur l'interface interne à destination de l'interface externe reçoit une traduction PAT NAT64 utilisant l'adresse IPv4 de l'interface externe.

Étape 3 Configurez la règle NAT46 statique pour le réseau IPv4 externe.

a) Cliquez sur le bouton +.

b) Configurez les propriétés suivantes :

- **Title** (Titre) = NAT46Rule (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = externe.
- **Interface de destination** = interne.
- **Original Address** (Adresse d'origine) = outside_v4_any network object.
- **Translated Address** (Adresse traduite) = inside_v6 network object.
- Dans l'onglet **Advanced Options** (Options avancées), sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle).



c) Cliquez sur **OK**.

Grâce à cette règle, toute adresse IPv4 du réseau externe acheminée à l'interface interne est traduite en adresse sur le réseau 2001:db8::/96 à l'aide de la méthode de l'adresse IPv4 intégrée. En outre, les réponses DNS des enregistrements A (IPv4) sont converties en enregistrements AAAA (IPv6) et les adresses IPv4 en IPv6.

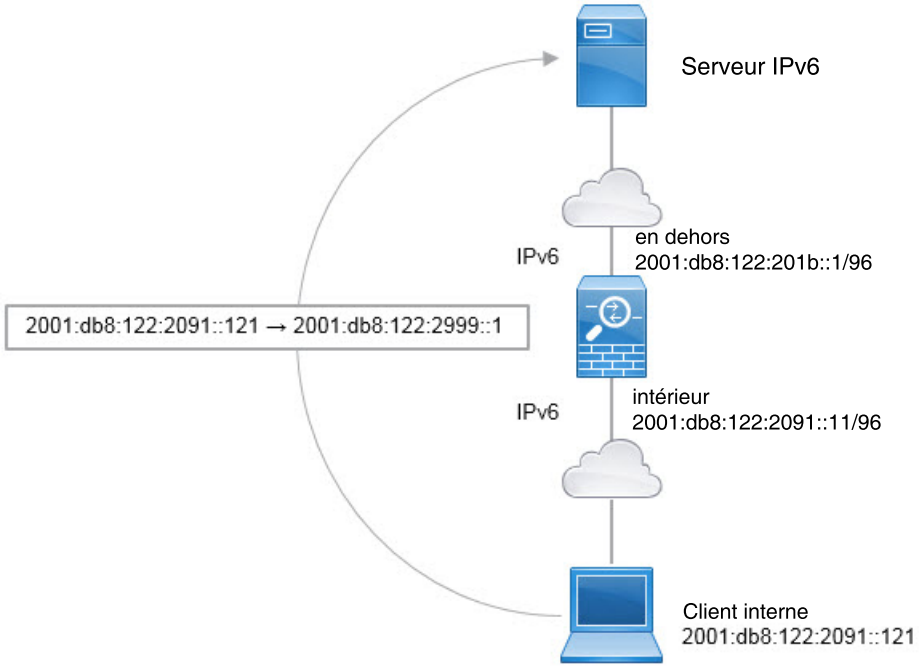
NAT66 : traduction d'adresses IPv6 en adresses différentes IPv6

Lorsque vous passe z d'un réseau IPv6 à un autre réseau IPv6, vous pouvez traduire les adresses en adresses IPv6 différentes sur le réseau externe. Nous vous recommandons d'utiliser la NAT statique. Bien que vous puissiez utiliser la NAT ou la PAT dynamique, les adresses IPv6 sont si nombreuses que vous n'êtes pas obligé d'utiliser la NAT dynamique.

Comme vous n'effectuez pas de traduction entre différents types d'adresses, vous n'avez besoin que d'une seule règle pour les traductions NAT66. Vous pouvez facilement modéliser ces règles à l'aide de auto NAT. Toutefois, si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle en utilisant uniquement NAT manuelle.

Exemple NAT66, de traduction statique entre réseaux

Vous pouvez configurer une traduction statique entre des regroupements d'adresses IPv6 en utilisant auto NAT. L'exemple suivant explique comment convertir des adresses internes sur le réseau 2001:db8:122:2091::/96 en adresses externes sur le réseau 2001:db8:122:2999::/96.



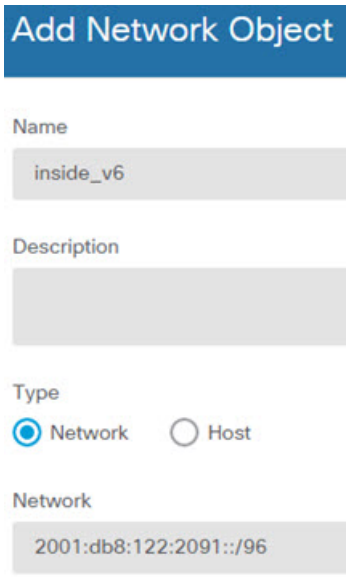
Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, vous devez dupliquer les règles pour chaque interface membre.

Procédure

Étape 1 Créez les objets réseau qui définissent les réseaux NAT IPv6 interne et externe.

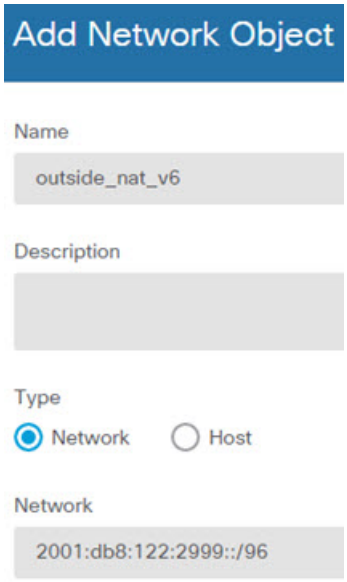
a) Choisissez **Objects** (Objets).
b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.
c) Définissez le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, inside_v6), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau, 2001:db8:122:2091::/96.



d) Cliquez sur **OK**.
e) Cliquez sur + et définissez le réseau NAT IPv6 externe.

Nommez l'objet réseau (par exemple, outside_nat_v6), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau 2001:db8:122:2999::/96.

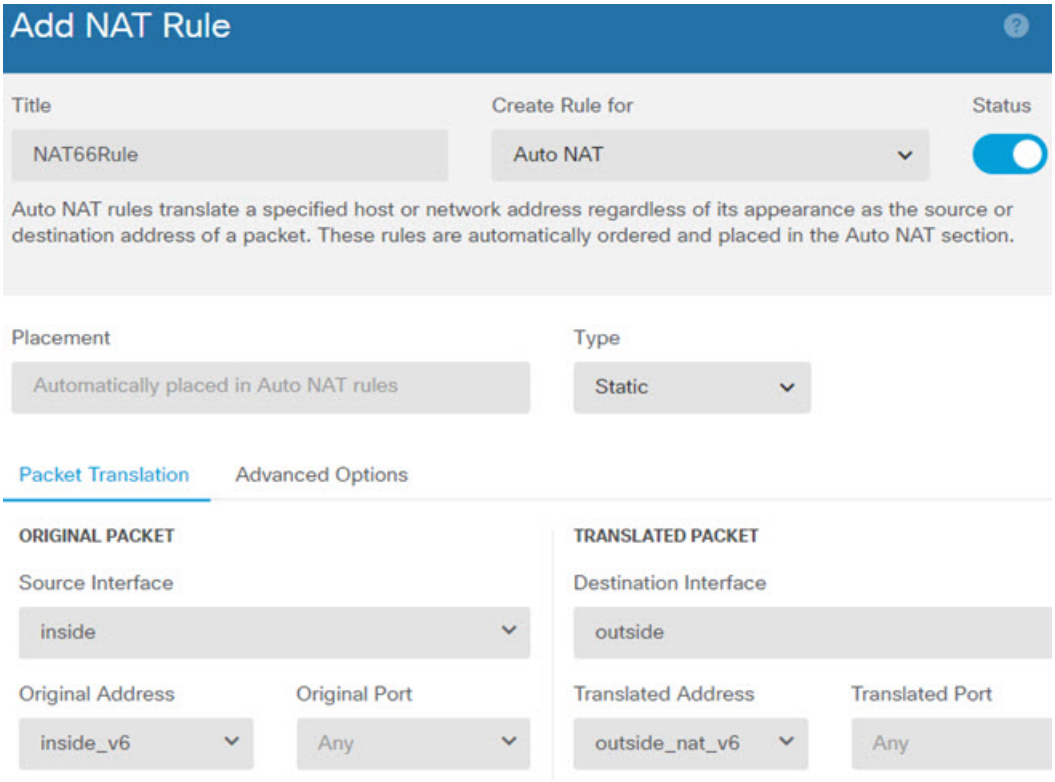


Étape 2 Configurez la règle NAT statique pour le réseau IPv6 interne.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton +.
c) Configurez les propriétés suivantes :

- **Titre** = NAT66Rule (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.

- **Type** = Statique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse originale** = inside_v6 network object.
- **Adresse traduite** = objet réseau outside_nat_v6.



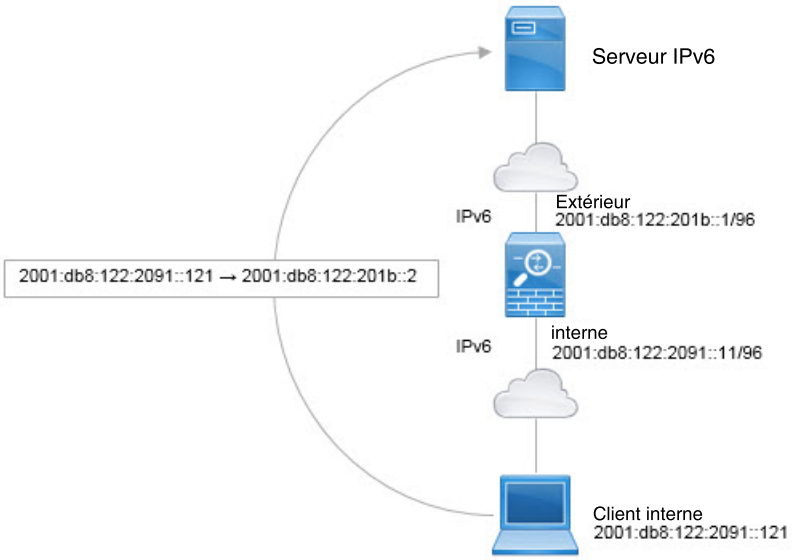
d) Cliquez sur **OK**.

Avec cette règle, tout trafic provenant du sous-réseau 2001:db8:122:2091::/96 sur l'interface interne vers l'interface externe reçoit une traduction NAT66 statique vers une adresse sur le réseau 2001:db8:122:2999::/96.

Exemple de NAT66, PAT d'interface IPv6 simple

Une approche simple pour la mise en œuvre de NAT66 consiste à affecter de manière dynamique des adresses internes à différents ports de l'adresse IPv6 de l'interface externe.

Cependant, vous ne pouvez pas configurer l'interface PAT en utilisant l'adresse IPv6 d'une interface à l'aide de la commande FDM. Au lieu de cela, utilisez une seule adresse libre sur le même réseau qu'un ensemble de PAT dynamique.



Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, vous devez dupliquer les règles pour chaque interface membre.

Procédure

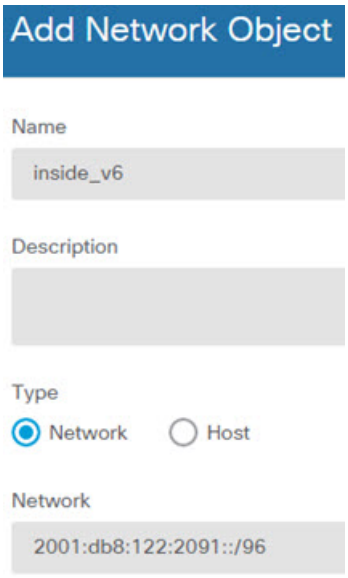
Étape 1 Créez les objets réseau qui définissent le réseau IPv6 interne et l'adresse IPv6 PAT.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur **+**.

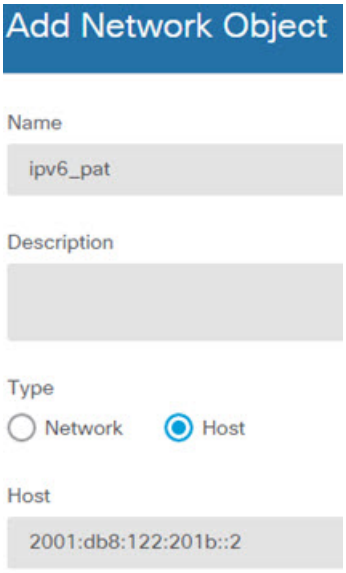
c) Définissez le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, inside_v6), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau, 2001:db8:122:2091::/96.



d) Cliquez sur **OK**.
e) Cliquez sur le signe + et définissez l'adresse PAT IPv6 externe.

Nommez l'objet réseau (par exemple, ipv6_pat), sélectionnez **Host** (Hôte) et saisissez l'adresse de l'hôte 2001:db8:122:201b::2.

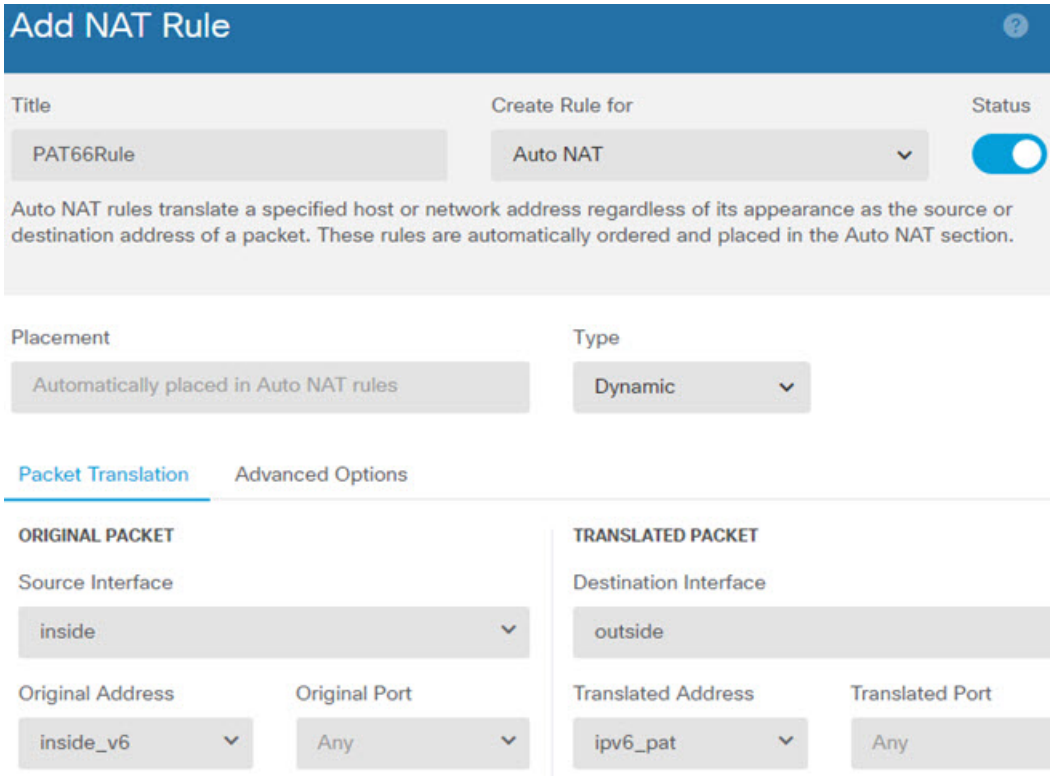


Étape 2 Configurez la règle PAT dynamique pour le réseau IPv6 interne.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton +.
c) Configurez les propriétés suivantes :

- **Title** (Titre) = PAT66Rule (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.

- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse originale** = inside_v6 network object.
- **Translated Address** (Adresse traduite) = ipv6_pat network object.



d) Cliquez sur **OK**.

Avec cette règle, tout trafic provenant du sous-réseau 2001:db8:122:2091::/96 sur l'interface interne vers l'interface externe reçoit une traduction dynamique PAT66 vers un port sur 2001:db8:122:201b::2.

Surveillance de la NAT

Pour surveiller et dépanner les connexions NAT, ouvrez la console de l'interface de ligne de commande ou connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes.

- **show nat** affiche les règles NAT et le nombre de résultats par règle. Il existe des mots-clés supplémentaires pour montrer d'autres aspects de la NAT.
- **show xlate** affiche les traductions NAT actuellement actives.

- **clear xlate** vous permet de supprimer une traduction NAT active. Vous devrez peut-être supprimer des traductions actives si vous modifiez les règles NAT, car les connexions existantes continuent d'utiliser l'ancien logement de traduction jusqu'à ce que la connexion se termine. L'effacement d'une traduction permet au système de créer une nouvelle traduction pour un client lors de la prochaine tentative de connexion du client en fonction de vos nouvelles règles. (Vous ne pouvez pas utiliser cette commande dans la console de l'interface de ligne de commande.)

Exemples relatifs à la NAT

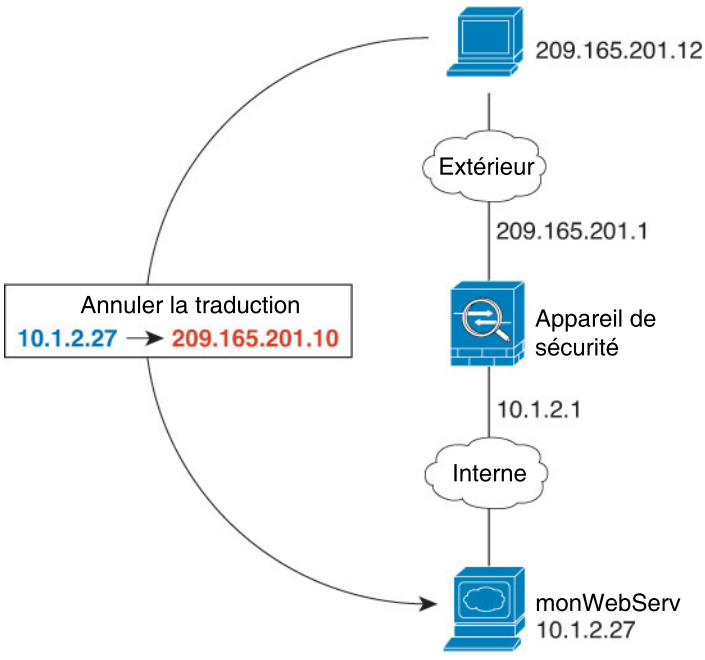
Les rubriques suivantes fournissent des exemples de configuration de la NAT sur les périphériques Threat Defense.

Fournir l'accès à un serveur Web interne (NAT automatique statique)

Dans l'exemple suivant, une NAT statique est effectuée pour un serveur Web interne. L'adresse réelle se trouve sur un réseau privé, une adresse publique est donc requise. Une NAT statique est nécessaire pour que les hôtes puissent initier le trafic vers le serveur Web à une adresse fixe.

Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, sélectionnez l'interface de membre du groupe de ponts à laquelle le serveur Web est relié, par exemple, inside1_3.

Illustration 21 : NAT statique pour un serveur Web interne



Procédure

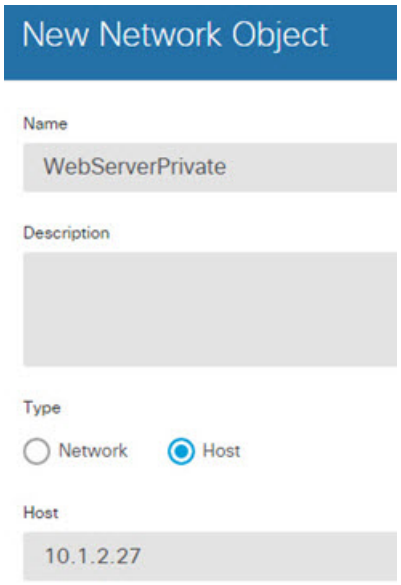
Étape 1 Créez les objets réseau qui définissent les adresses d'hôte privées et publiques du serveur.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.

c) Définissez l'adresse privée du serveur Web.

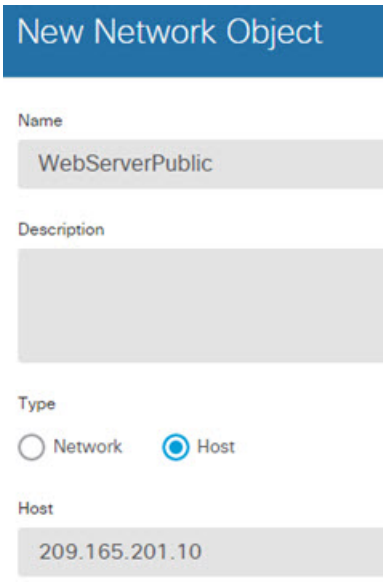
Nommez l'objet réseau (par exemple, WebServerPrivate), sélectionnez **Host** (Hôte), et saisissez l'adresse IP réelle de l'hôte, 10.1.2.27.



d) Cliquez sur **OK**.

e) Cliquez sur + et définissez l'adresse publique.

Nommez l'objet réseau (par exemple, WebServerPublic), sélectionnez **Host** (Hôte), et saisissez l'adresse de l'hôte 209.165.201.10.

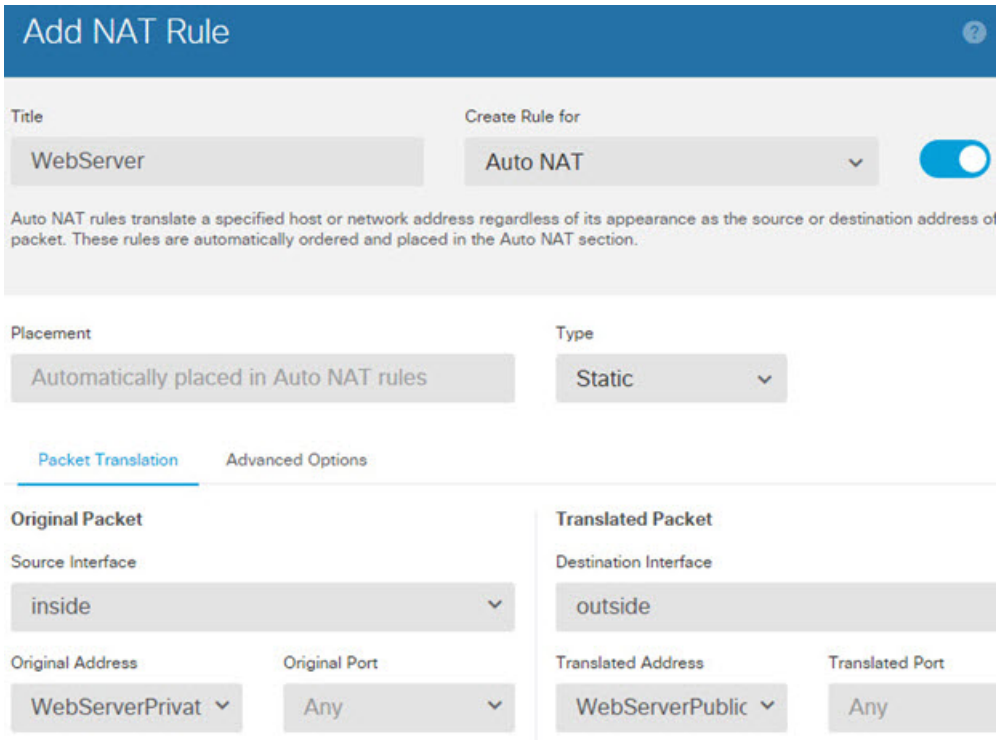


f) Cliquez sur **OK**.

Étape 2 Configurez la NAT statique pour l'objet

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton +.
c) Configurez les propriétés suivantes :

- **Titre** = WebServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Original Address (**Adresse d'origine) = objet réseau WebServerPrivate.
- **Translated Address** (Adresse traduite) = objet réseau WebServerPublic.



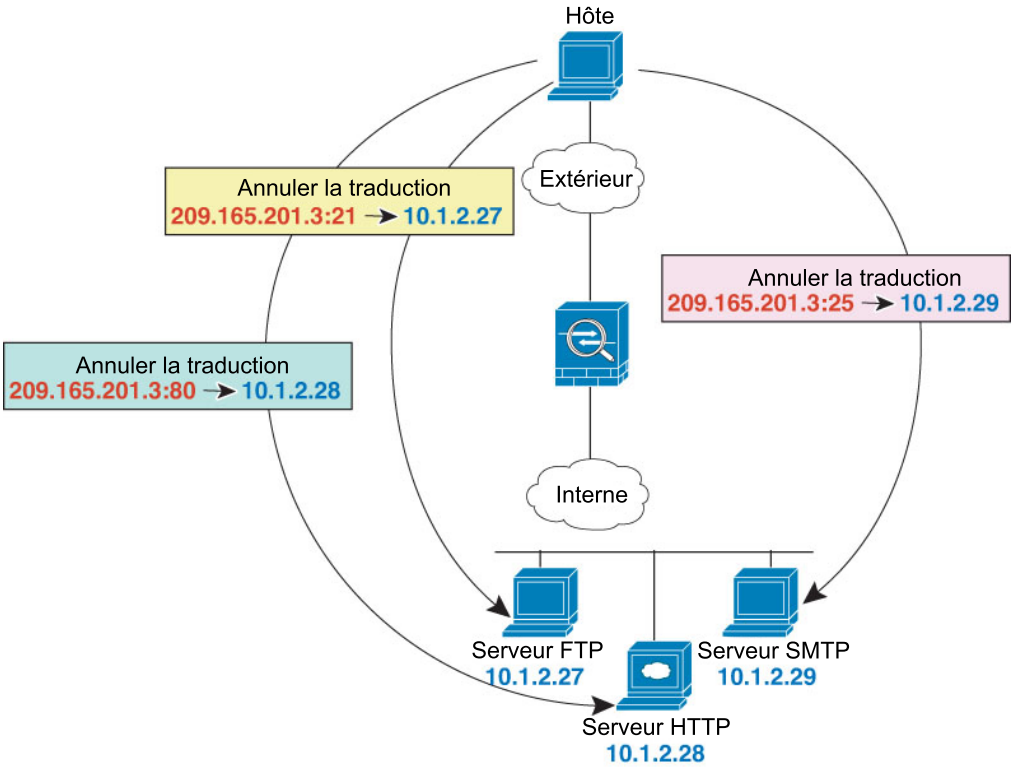
d) Cliquez sur **OK**.

Adresse unique pour FTP, HTTP et SMTP (NAT automatique statique avec traduction de port)

L'exemple de NAT statique avec traduction de port statique suivant fournit une adresse unique permettant aux utilisateurs distants d'accéder à FTP, HTTP et SMTP. Ces serveurs sont en fait des périphériques différents sur le réseau réel, mais pour chaque serveur, vous pouvez spécifier des règles NAT statiques avec des règles de traduction de port qui utilisent la même adresse IP mappée, mais des ports différents.

Remarque Cet exemple suppose que l'interface interne est une interface routée standard connectée à un commutateur, avec les serveurs connectés au commutateur. Si votre interface interne est une interface de groupe de ponts (BVI) et que les serveurs sont associés à des interfaces de membre de groupe de ponts distinctes, sélectionnez l'interface de membre spécifique à laquelle chaque serveur est associé pour la règle correspondante. Par exemple, les règles peuvent avoir inside1_2, inside1_3 et inside1_4 pour l'interface source plutôt que inside.

Illustration 22 : NAT statique avec traduction de port



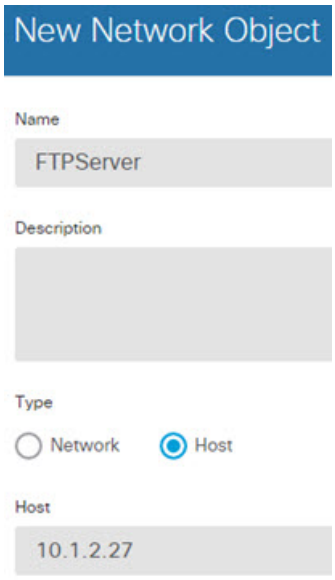
Procédure

Étape 1 Créez un objet réseau pour le serveur FTP.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.

c) Nommez l'objet réseau (par exemple, FTPserver), sélectionnez **Host** (Hôte), et saisissez l'adresse IP réelle du serveur FTP, 10.1.2.27.

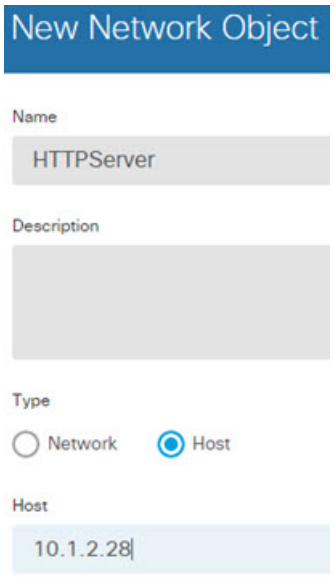


d) Cliquez sur **OK**.

Étape 2 Créez un objet réseau pour le serveur HTTP.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, HTTPserver), sélectionnez **Host** (Hôte), et saisissez l'adresse d'hôte 10.1.2.28.

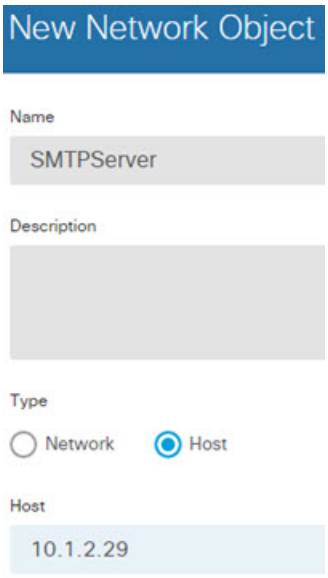


c) Cliquez sur **OK**.

Étape 3 Créez un objet réseau pour le serveur SMTP.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, SMTPserver), sélectionnez **Host (Hôte)**, et saisissez l'adresse d'hôte 10.1.2.29.

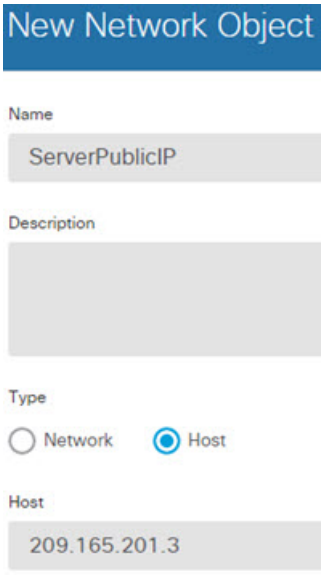


c) Cliquez sur **OK**.

Étape 4 Créez un objet réseau pour l'adresse IP publique utilisée pour les trois serveurs.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, ServerPublicIP), sélectionnez **Host** (Hôte), et saisissez l'adresse d'hôte 209.165.201.3.



c) Cliquez sur **OK**.

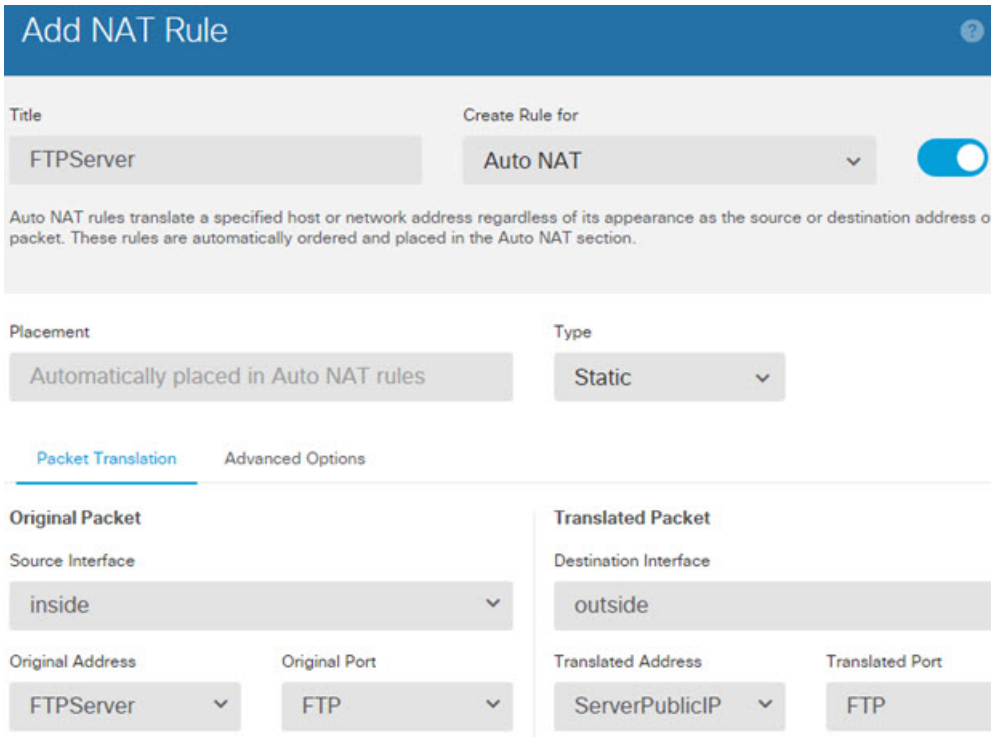
Étape 5 Configurez la NAT statique avec la traduction de port pour le serveur FTP, en mappant le port FTP sur lui-même.

a) Sélectionnez **Policies (Politiques)** > **NAT**.

b) Cliquez sur le bouton +.

c) Configurez les propriétés suivantes :

- **Titre** = FTPServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse d'origine** = objet réseau FTPserver.
- **Adresse traduite** = objet réseau ServerPublicIP.
- **Port d'origine** = objet de port FTP.
- **Port traduit** = objet de port FTP.



d) Cliquez sur **OK**.

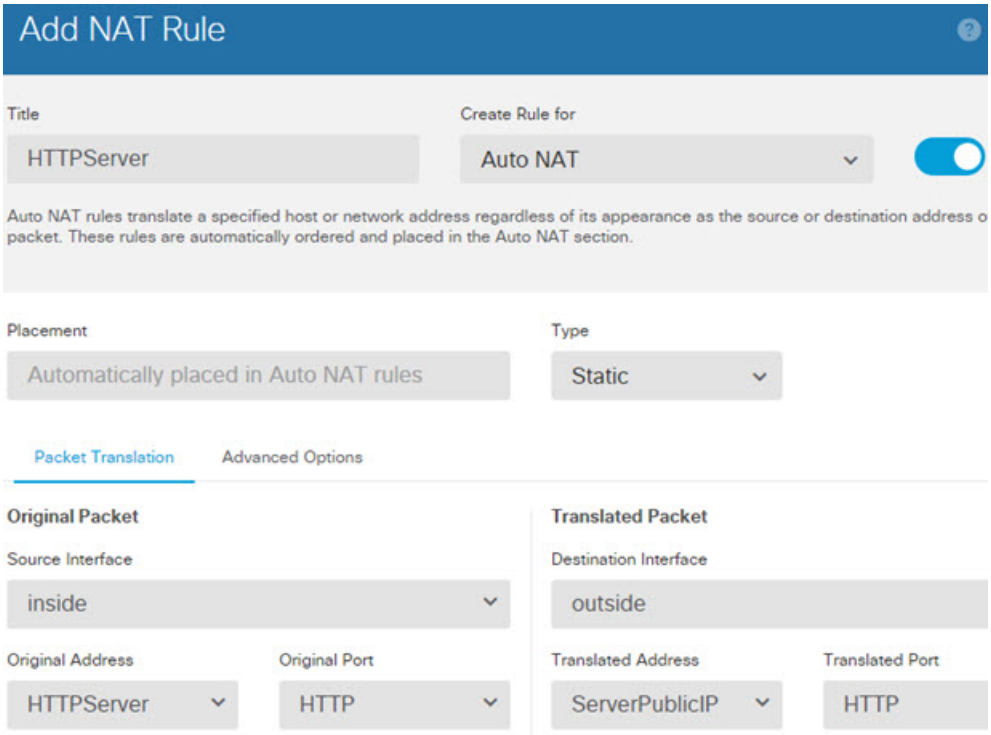
Étape 6 Configurez la NAT statique avec la traduction de port pour le serveur HTTP, en mappant le port HTTP sur lui-même.

a) Cliquez sur le bouton **+**.

b) Configurez les propriétés suivantes :

- **Titre** = HTTPServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = interne.

- **Interface de destination** = externe.
- **Adresse d'origine** = objet réseau HTTPserver.
- **Adresse traduite** = objet réseau ServerPublicIP.
- **Port d'origine** = objet de port HTTP.
- **Port traduit** = objet de port HTTP.



c) Cliquez sur **OK**.

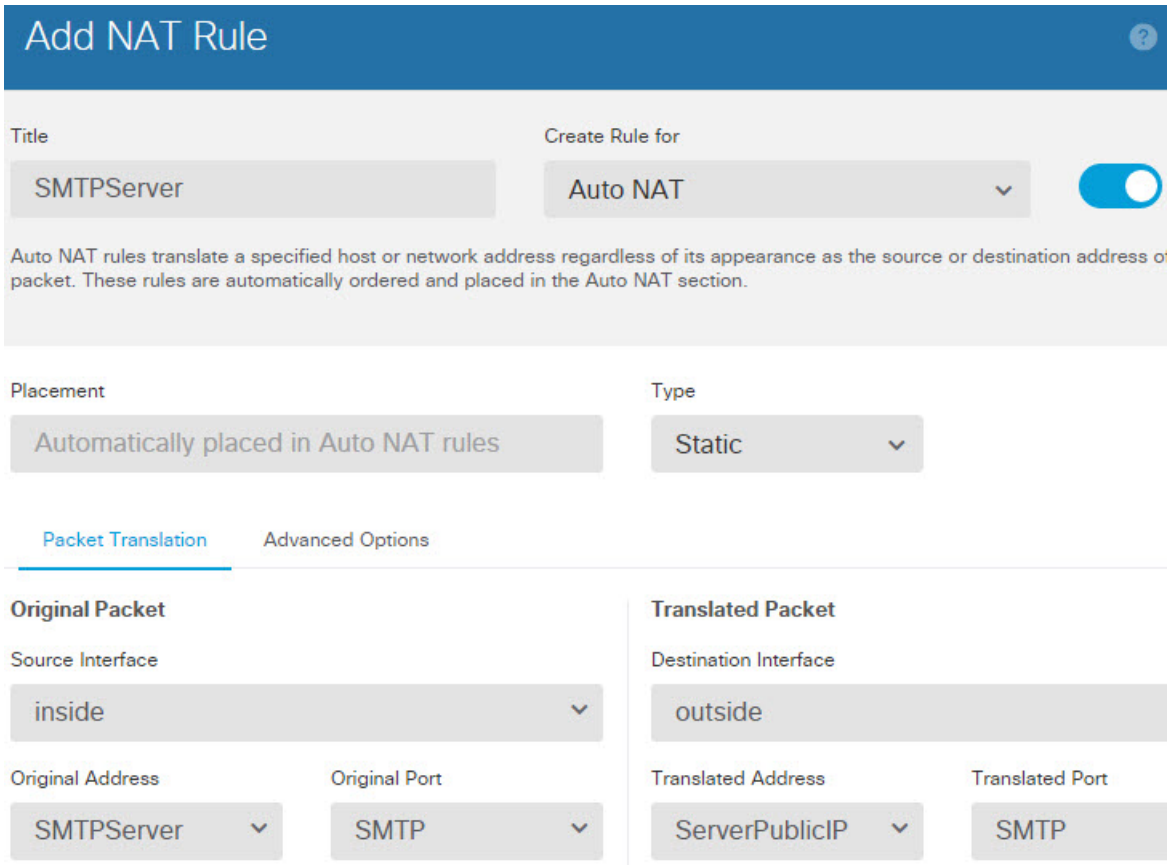
Étape 7 Configurez la NAT statique avec la traduction de port pour le serveur SMTP, en mappant le port SMTP sur lui-même.

a) Cliquez sur le bouton +.

b) Configurez les propriétés suivantes :

- **Titre** = SMTPServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse d'origine** = objet réseau du serveur SMTP.
- **Adresse traduite** = objet réseau ServerPublicIP.
- **Port d'origine** = objet de port SMTP.

- **Port traduit** = objet de port SMTP.



c) Cliquez sur **OK**.

Traduction différente selon la destination (PAT manuelle dynamique)

La figure suivante montre un hôte sur le réseau 10.1.2.0/24 accédant à deux serveurs différents. Lorsque l'hôte accède au serveur par l'adresse 209.165.201.11, l'adresse réelle est traduite en 209.165.202.129 :*port*. Lorsque l'hôte accède au serveur à partir de l'adresse 209.165.200.225, l'adresse réelle est traduite en 209.165.202.130 :*port*.

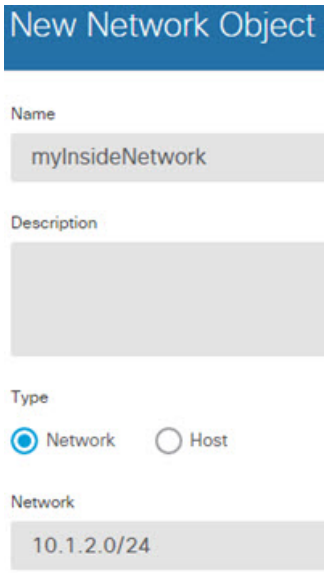
Remarque Cet exemple suppose que l'interface interne est une interface routée standard connectée à un commutateur, avec les serveurs connectés au commutateur. Si votre interface interne est une interface de groupe de ponts (BVI) et que les serveurs sont associés à des interfaces de membre de groupe de ponts distinctes, sélectionnez l'interface de membre spécifique à laquelle chaque serveur est associé pour la règle correspondante. Par exemple, les règles peuvent avoir interne1_2 et interne1_3 pour l'interface source plutôt que interne.

Illustration 23 : NAT manuelle avec différentes adresses de destination

Procédure

Étape 1 Créez un objet réseau pour le réseau interne.

a) Choisissez **Objects** (Objets).
b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur **+**.
c) Nommez l'objet réseau (par exemple, myInsideNetwork), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau réelle, soit 10.1.2.0/24.

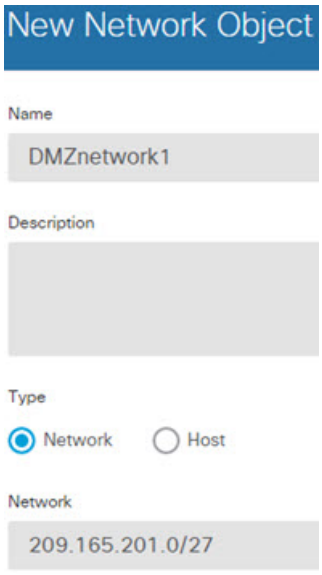


d) Cliquez sur **OK**.

Étape 2 Créer un objet réseau pour le réseau DMZ 1.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, DMZnetwork1), sélectionnez **Network (Réseau)**, et saisissez l'adresse réseau 209.165.201.0/27 (masque de sous-réseau 255.255.255.224).

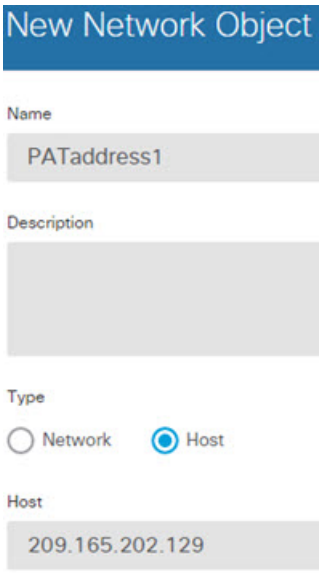


c) Cliquez sur **OK**.

Étape 3 Créez un objet réseau pour l'adresse PAT du réseau DMZ 1.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, PATaddress1), sélectionnez **Host** (Hôte), et saisissez l'adresse d'hôte 209.165.202.129.

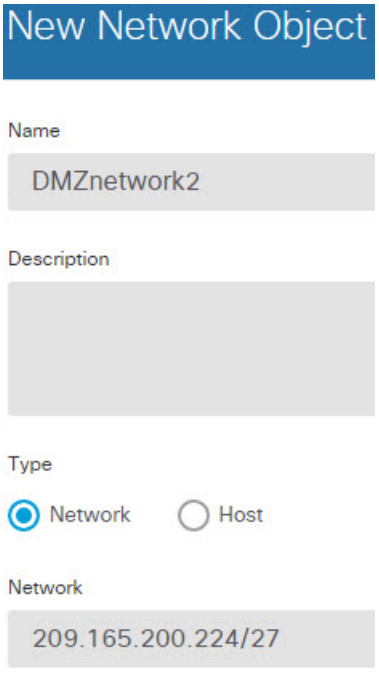


c) Cliquez sur **OK**.

Étape 4 Créez un objet réseau pour le réseau DMZ 2.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, DMZnetwork2), sélectionnez **Network (Réseau)**, et saisissez l'adresse réseau 209.165.201.0/27 (masque de sous-réseau 255.255.255.224).

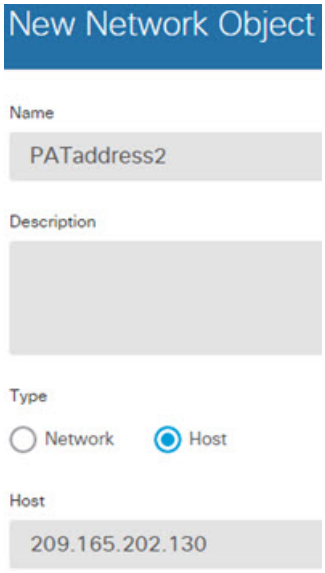


c) Cliquez sur **OK**.

Étape 5 Créez un objet réseau pour l'adresse PAT du réseau DMZ 2.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, PATaddress2), sélectionnez **Host (Hôte)**, et saisissez l'adresse d'hôte 209.165.202.130.



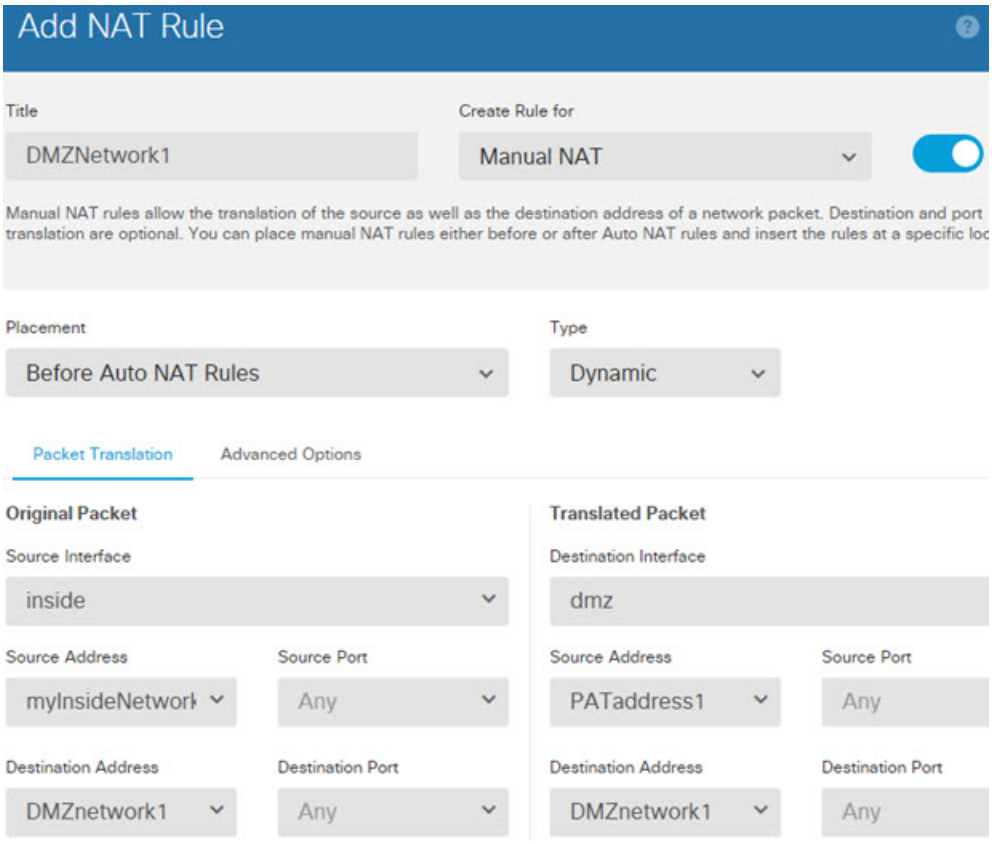
c) Cliquez sur **OK**.

Étape 6 Configurez la PAT manuelle dynamique pour le réseau DMZ 1.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton **+**.
c) Configurez les propriétés suivantes :

- **Title** (Titre) = DMZNetwork1 (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = dmz.
- **Original Source Address** (Adresse source d'origine) = objet de réseau myInsideNetwork.
- Adresse **source traduite** = objet de réseau PATaddress1.
- **Adresse de destination d'origine** = objet réseau DMZnetwork1.
- **Adresse de destination traduite** = objet réseau DMZnetwork1.

Remarque
Comme vous ne souhaitez pas traduire l'adresse de destination, vous devez configurer la NAT d'identité en utilisant la même adresse pour les adresses de destination originale et traduite. Laissez tous les champs de port vides.



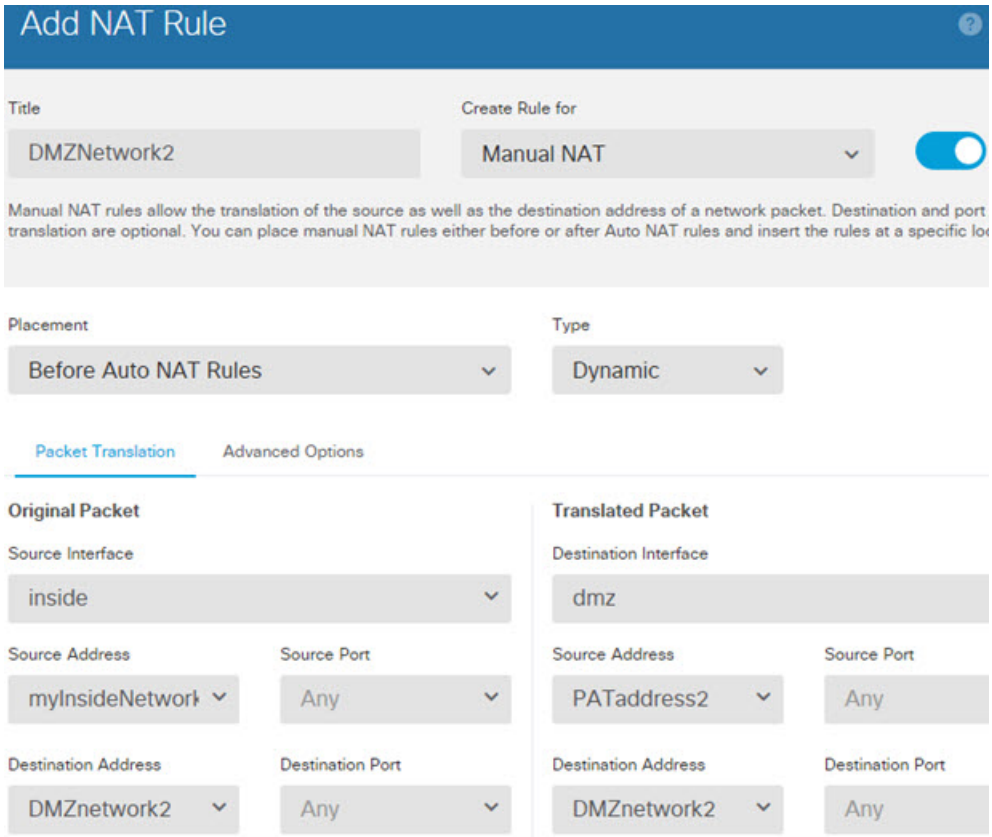
d) Cliquez sur **OK**.

Étape 7 Configurez la PAT manuelle dynamique pour le réseau DMZ 2.

a) Cliquez sur le bouton +.

b) Configurez les propriétés suivantes :

- **Title** (Titre) = DMZNetwork2 (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = dmz.
- **Original Source Address** (Adresse source d'origine) = objet de réseau myInsideNetwork.
- **Translated Source Address** (Adresse source traduite) = objet de réseau PATaddress2.
- **Adresse de destination d'origine** = objet réseau DMZnetwork2.
- **Adresse de destination traduite** = objet réseau DMZnetwork2.



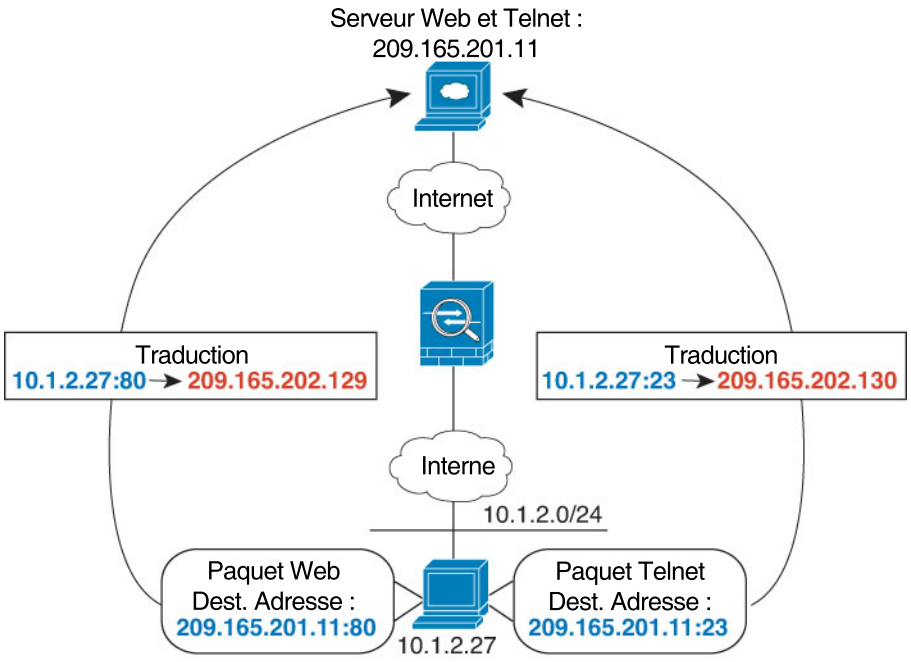
c) Cliquez sur **OK**.

Traduction différente selon l'adresse et le port de destination (PAT manuelle dynamique)

La figure suivante montre l'utilisation des ports source et de destination. L'hôte du réseau 10.1.2.0/24 accède à un hôte unique pour les services Web et Telnet. Lorsque l'hôte accède au serveur pour les services Telnet, l'adresse réelle est traduite en 209.165.202.129 :*port*. Lorsque l'hôte accède au même serveur pour les services Web, l'adresse réelle est traduite par 209.165.202.130 :*port*.

Remarque Cet exemple suppose que l'interface interne est une interface routée standard connectée à un commutateur, avec le serveur connecté au commutateur. Si votre interface interne est une interface de groupe de ponts (BVI) et que le serveur est associé à une interface de membre de groupe de ponts, sélectionnez l'interface de membre spécifique à laquelle le serveur est associé. Par exemple, la règle peut avoir inside1_2 pour l'interface source plutôt que inside.

Illustration 24 : NAT manuelle avec différents ports de destination



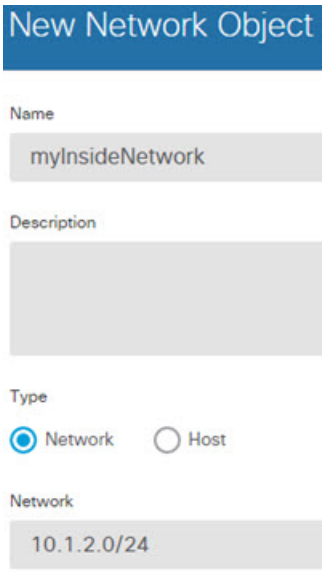
Procédure

Étape 1 Créez un objet réseau pour le réseau interne.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur **+**.

c) Nommez l'objet réseau (par exemple, myInsideNetwork), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau réelle, soit 10.1.2.0/24.

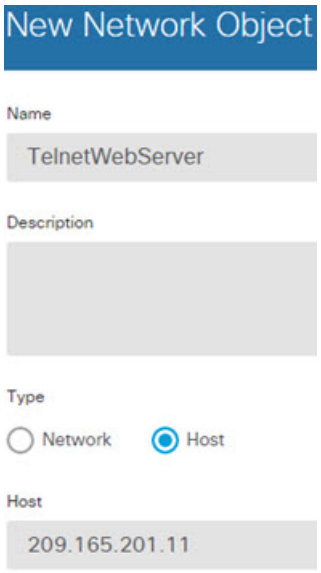


d) Cliquez sur **OK**.

Étape 2 Créez un objet réseau pour le serveur Telnet/Web.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, TelnetWebServer), sélectionnez **Host** (Hôte), et saisissez l'adresse d'hôte 209.165.201.11.

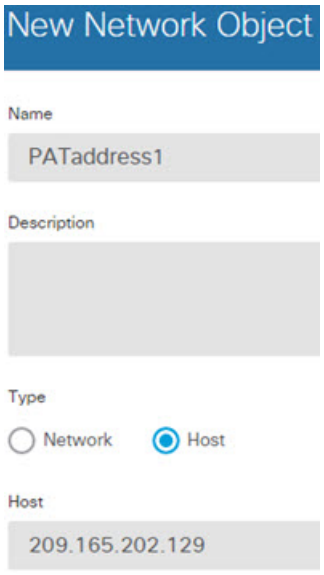


c) Cliquez sur **OK**.

Étape 3 Créez un objet réseau pour l'adresse PAT lorsque vous utilisez Telnet.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, PATaddress1), sélectionnez **Host** (Hôte), et saisissez l'adresse d'hôte 209.165.202.129.

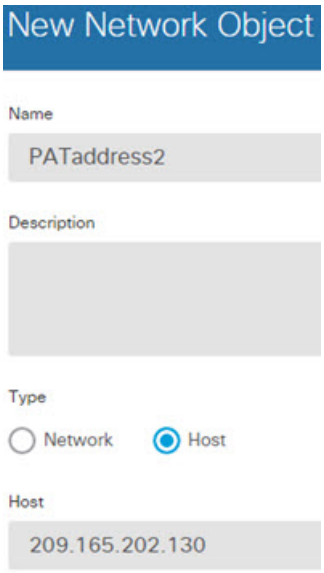


c) Cliquez sur **OK**.

Étape 4 Créez un objet réseau pour l'adresse PAT lorsque vous utilisez HTTP.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, PATaddress2), sélectionnez **Host (Hôte)**, et saisissez l'adresse d'hôte 209.165.202.130.



c) Cliquez sur **OK**.

Étape 5 Configurez la PAT manuelle dynamique pour l'accès Telnet.

a) Sélectionnez **Policies (Politiques)** > **NAT**.

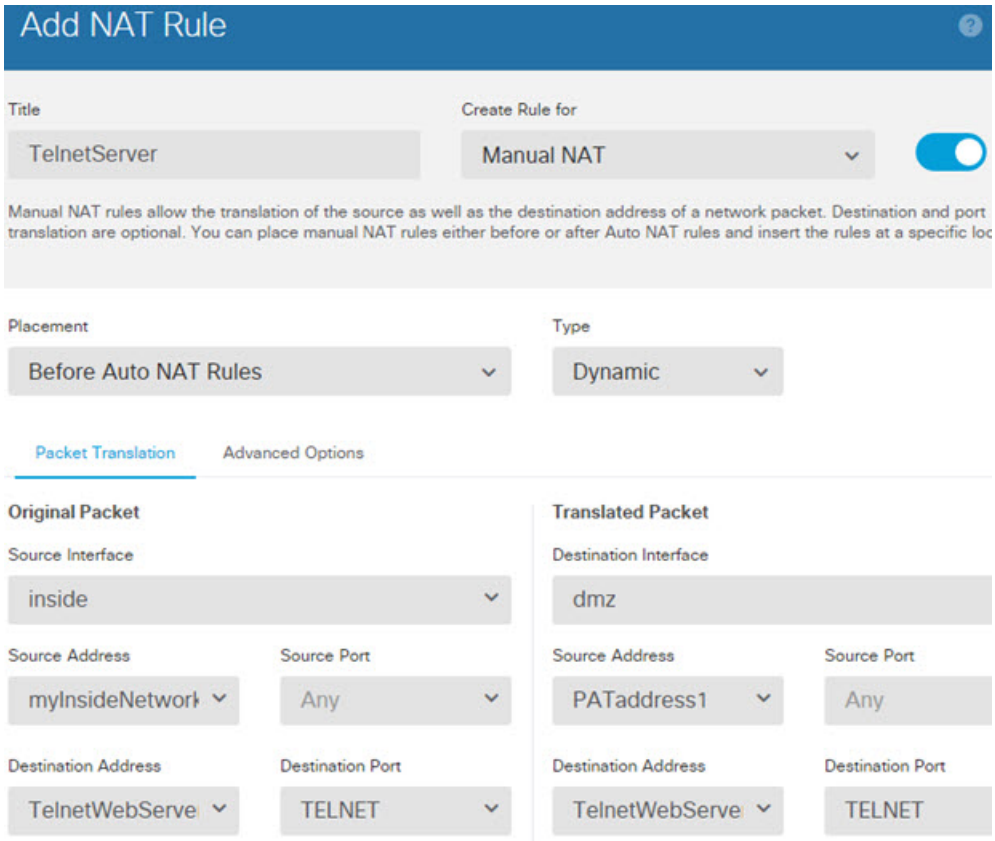
b) Cliquez sur le bouton +.

c) Configurez les propriétés suivantes :

- **Title** (Titre) = TelnetServer (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = dmz.
- **Original Source Address** (Adresse source d'origine) = objet de réseau myInsideNetwork.
- **Translated Source Address** (Adresse source traduite) = objet de réseau PATaddress1.
- **Original Destination Address**s (Adresse de destination d'origine) = objet réseau TelnetWebServer.
- **Translated Destination Address** (Adresse de destination traduite) = objet réseau TelnetWebServer.
- **Original Destination Port** (Port de destination d'origine) = objet de port TELNET.
- **Translated Destination Port** (Port de destination traduit) = objet de port TELNET.

Remarque

Comme vous ne souhaitez pas traduire l'adresse ou le port de destination, vous devez configurer la NAT d'identité pour cette adresse en spécifiant la même adresse pour les adresses de destination d'origine et traduites, et le même port pour le port d'origine et traduit.



d) Cliquez sur **OK**.

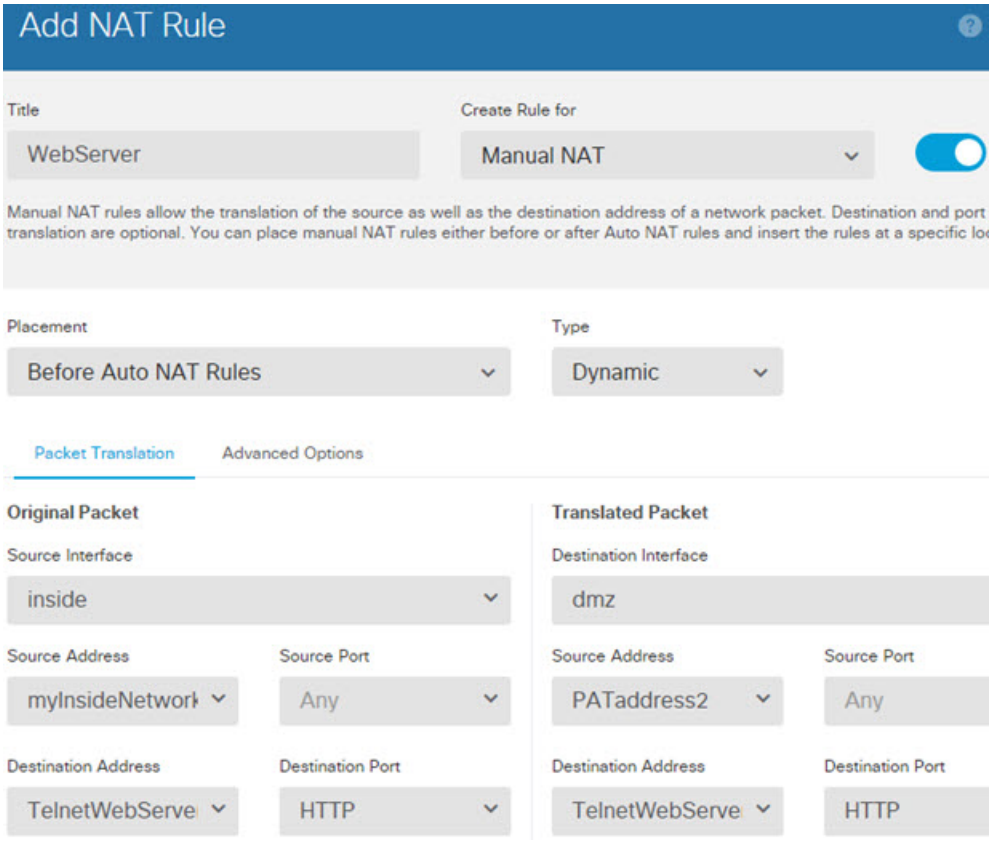
Étape 6 Configurez la PAT manuelle dynamique pour l'accès Web.

a) Cliquez sur le bouton **+**.

b) Configurez les propriétés suivantes :

- **Titre** = WebServer (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = dmz.
- **Original Source Address** (Adresse source d'origine) = objet de réseau myInsideNetwork.
- **Translated Source Address** (Adresse source traduite) = objet de réseau PATaddress2.
- **Original Destination Addres**s (Adresse de destination d'origine) = objet réseau TelnetWebServer.
- **Translated Destination Address** (Adresse de destination traduite) = objet réseau TelnetWebServer.

- **Original Destination Port** (Port de destination d'origine) = objet de port HTTP.
- **Translated Destination Port** (Port de destination traduit) = objet de port HTTP.



c) Cliquez sur **OK**.

Réécriture des requêtes et des réponses DNS à l'aide de la NAT

Vous devrez peut-être configurer Appareil FTD pour modifier les réponses DNS en remplaçant l'adresse dans la réponse par une adresse qui correspond à la configuration NAT. Vous pouvez configurer la modification DNS lorsque vous configurez chaque règle de traduction. La modification DNS est également connue sous le nom de contrôle DNS.

Cette fonctionnalité réécrit l'adresse dans les requêtes DNS et les réponses qui correspondent à une règle NAT (par exemple, l'enregistrement A pour IPv4, l'enregistrement AAAA pour IPv6 ou l'enregistrement PTR pour les requêtes DNS inversées). Pour les réponses DNS passant d'une interface mappée à toute autre interface, l'enregistrement est réécrit de la valeur mappée à la valeur réelle. Inversement, pour les réponses DNS traversant une interface vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette fonctionnalité fonctionne avec NAT44, NAT 66, NAT46 et NAT64.

Voici les principales circonstances dans lesquelles vous devez configurer la réécriture DNS sur une règle NAT.

- La règle est NAT64 ou NAT46 et le serveur DNS se situe sur le réseau externe. Vous devez réécrire le DNS pour convertir les enregistrements DNS A (pour IPv4) et les enregistrements AAAA (pour IPv6).
- Le serveur DNS est à l'extérieur, les clients sont à l'intérieur et certains des noms de domaine complets que les clients utilisent mènent aux autres hôtes internes.
- Le serveur DNS est à l'intérieur et répond par des adresses IP privées, les clients sont à l'extérieur et les clients accèdent aux noms de domaine complets qui pointent vers des serveurs hébergés à l'intérieur.

Limites de la réécriture DNS

Voici quelques limites concernant la réécriture DNS :

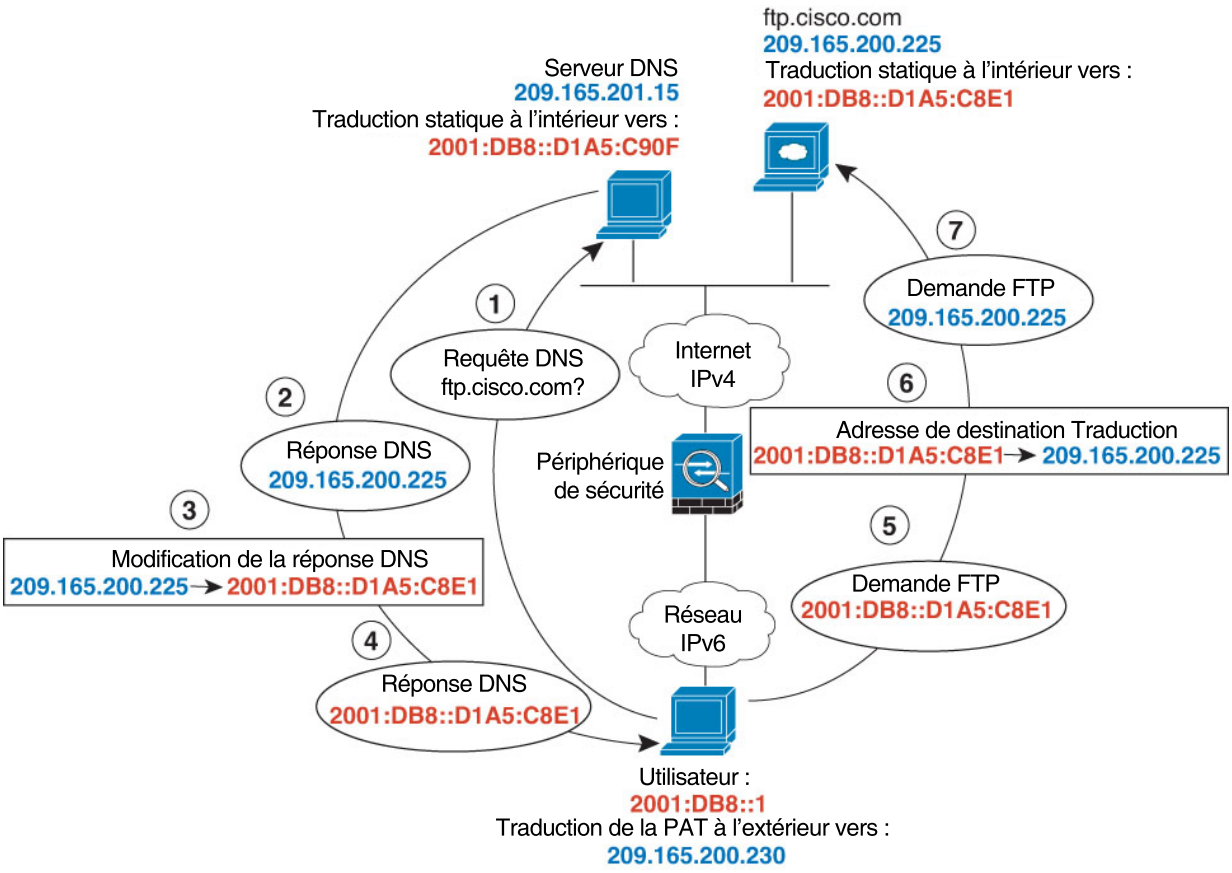
- La réécriture DNS ne s'applique pas à la PAT, car plusieurs règles PAT sont applicables pour chaque enregistrement A ou AAAA et que la règle PAT à privilégier est ambiguë.
- Si vous configurez une règle NAT manuelle, vous ne pouvez pas configurer la modification DNS si vous spécifiez l'adresse de destination ainsi que l'adresse source. Ces types de règles sont susceptibles d'être assorties d'une traduction différente pour une adresse unique lorsqu'on passe à A par rapport à B. Par conséquent, ne peut pas faire correspondre avec précision l'adresse IP à l'intérieur de la réponse DNS à la règle NAT double exacte; la réponse DNS ne contient pas d'information sur la combinaison d'adresses source/destination dans le paquet qui a déclenché la demande DNS.
- En fait, la réécriture DNS s'effectue sur l'entrée xlate, et non sur la règle NAT. Ainsi, s'il n'y a pas de xlate pour une règle dynamique, la réécriture ne peut pas s'effectuer correctement. Le même problème ne se produit pas pour la NAT statique.
- La réécriture DNS ne réécrit pas les messages de mise à jour dynamique DNS (opcode 5).

Les rubriques suivantes présentent des exemples de réécriture DNS dans les règles NAT.

Modification de la réponse DNS64

La figure suivante montre un serveur FTP et un serveur DNS sur le réseau IPv4 externe. Le système dispose d'une traduction statique pour le serveur externe. Dans ce cas, quand un utilisateur IPv6 interne demande l'adresse de ftp.cisco.com au serveur DNS, ce dernier répond par l'adresse réelle, 209.165.200.225.

Comme vous souhaitez que les utilisateurs internes utilisent l'adresse mappée pour ftp.cisco.com (2001:DB8::D1A5:C8E1, où D1A5:C8E1 est l'équivalent IPv6 de 209.165.200.225), vous devez configurer la modification de la réponse DNS pour la traduction statique. Cet exemple comprend également une traduction NAT statique pour le serveur DNS et une règle PAT pour les hôtes IPv6 internes.



Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, vous devez dupliquer les règles pour chaque interface membre.

Procédure

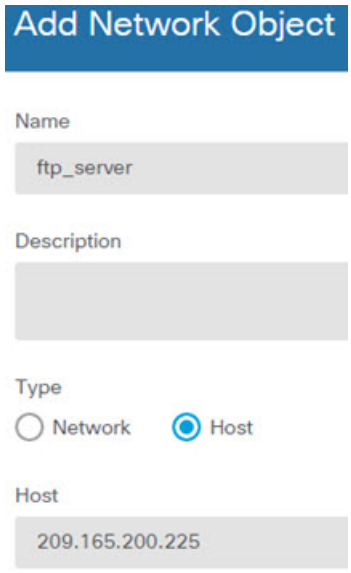
Étape 1 Créez les objets réseau pour le serveur FTP, le serveur DNS, le réseau interne et l'ensemble PAT.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.

c) Définissez l'adresse réelle du serveur FTP.

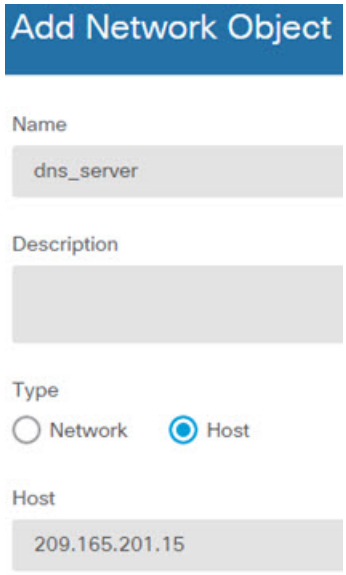
Nommez l'objet réseau (par exemple, ftp_server), sélectionnez **Host** (Hôte), et saisissez l'adresse IP réelle de l'hôte, 209.165.200.225.



d) Cliquez sur **OK**.

e) Cliquez sur + et définissez l'adresse réelle du serveur DNS.

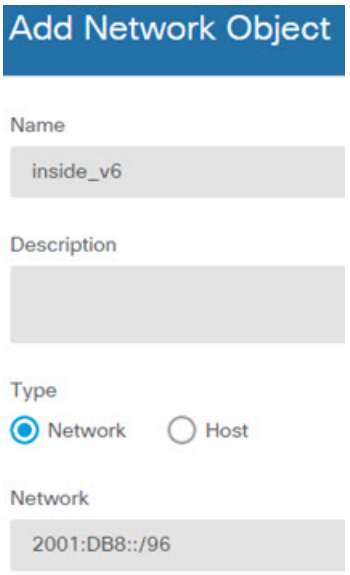
Nommez l'objet réseau (par exemple, dns_server), sélectionnez **Host** (Hôte), et saisissez l'adresse de l'hôte, 209.165.201.15.



f) Cliquez sur **OK**.

g) Cliquez sur + et définissez le réseau IPv6 interne.

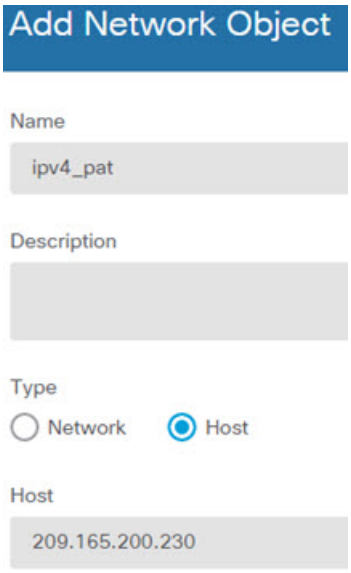
Nommez l'objet réseau (par exemple, inside_v6), sélectionnez **Network** (réseau), puis saisissez l'adresse réseau 2001:DB8::/96.



h) Cliquez sur **OK**.

i) Cliquez sur + et définissez l'adresse PAT IPv4 pour le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, ipv4_pat), sélectionnez **Host** (Hôte), et saisissez l'adresse de l'hôte, 209.165.200.230.



j) Cliquez sur **OK**.

Étape 2 Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

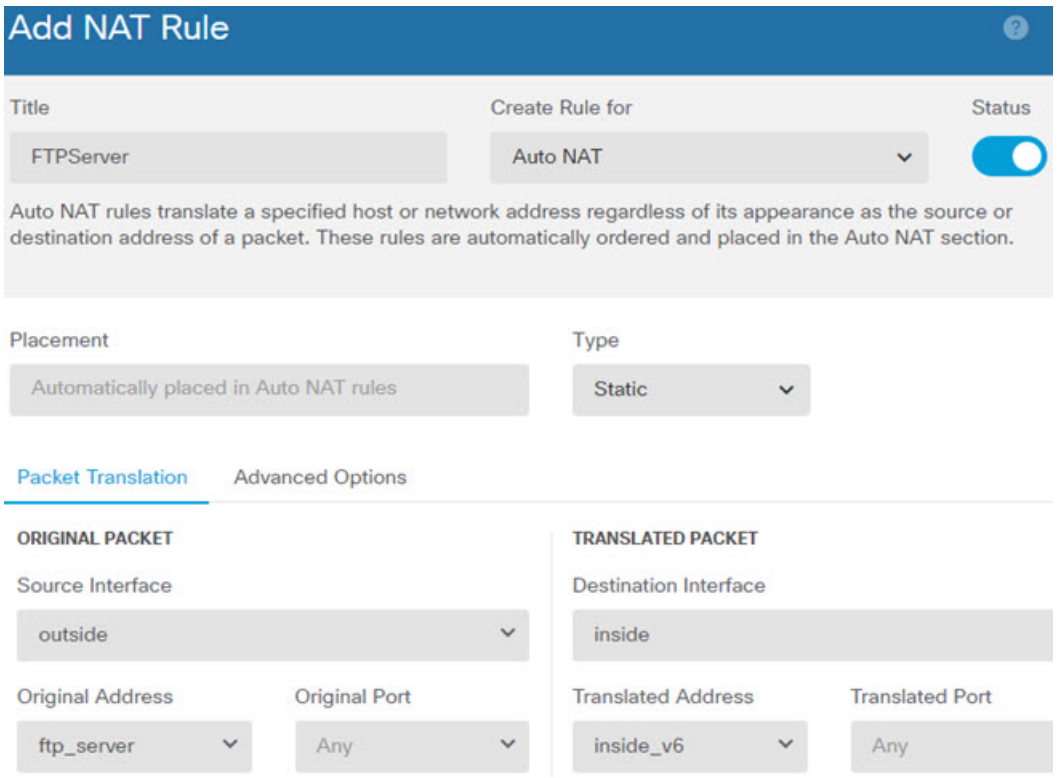
a) Sélectionnez **Policies (Politiques)** > **NAT**.

b) Cliquez sur le bouton +.

c) Configurez les propriétés suivantes :

- **Titre** = FTPServer (ou un autre nom de votre choix).

- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = externe.
- **Interface de destination** = interne.
- **Adresse d'origine** = objet réseau ftp_server.
- **Adresse traduite** = objet réseau inside_v6. Comme la méthode d'adresse intégrée IPv4 est utilisée lors de la conversion d'IPv4 en adresses IPv6, 209.165.200.225 est converti en équivalent IPv6 D1A5:C8E1 et le préfixe de réseau est ajouté pour obtenir l'adresse complète, 2001:DB8::D1A5:C8E1.
- Dans l'onglet **Advanced Options** (Options avancées), sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle).



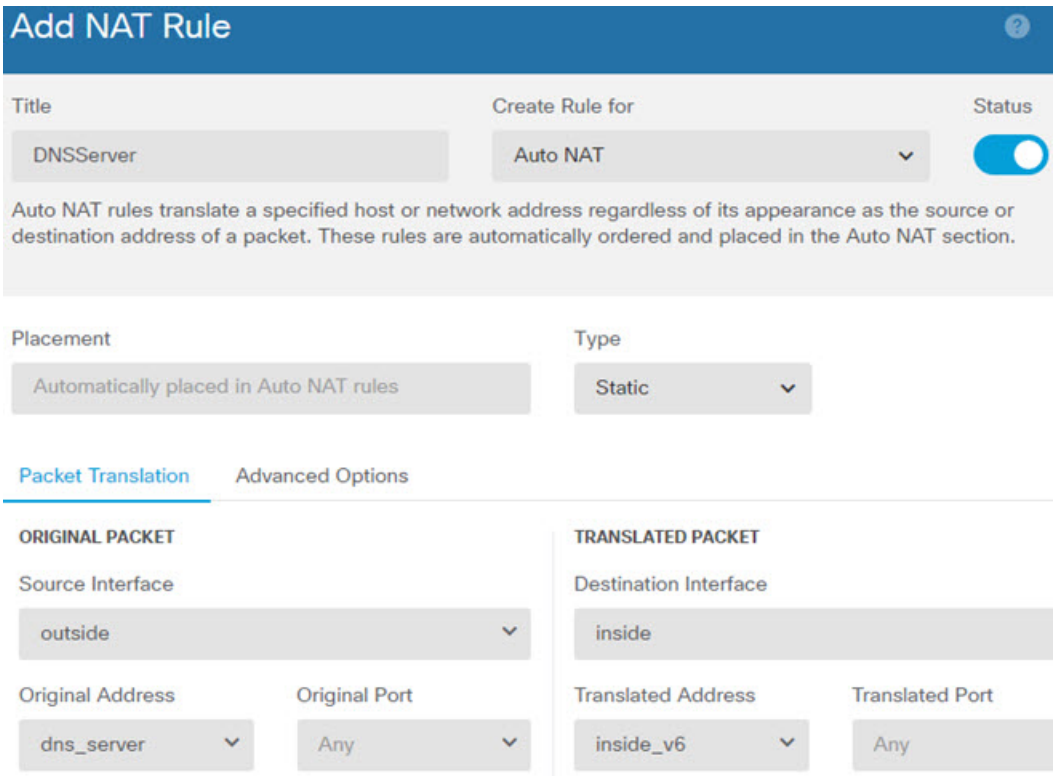
d) Cliquez sur **OK**.

Étape 3 Configurez la règle NAT statique pour le serveur DNS.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton **+**.
c) Configurez les propriétés suivantes :

- **Titre** = DNSServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.

- **Interface source** = externe.
- **Interface de destination** = interne.
- **Adresse d'origine** = objet réseau dns_server.
- **Adresse traduite** = objet réseau inside_v6. Comme la méthode d'adresse intégrée IPv4 est utilisée lors de la conversion d'IPv4 en adresses IPv6, 209.165.201.15 est converti en équivalent IPv6 D1A5:C90F et le préfixe de réseau est ajouté pour obtenir l'adresse complète, 2001:DB8::D1A5:C90F.

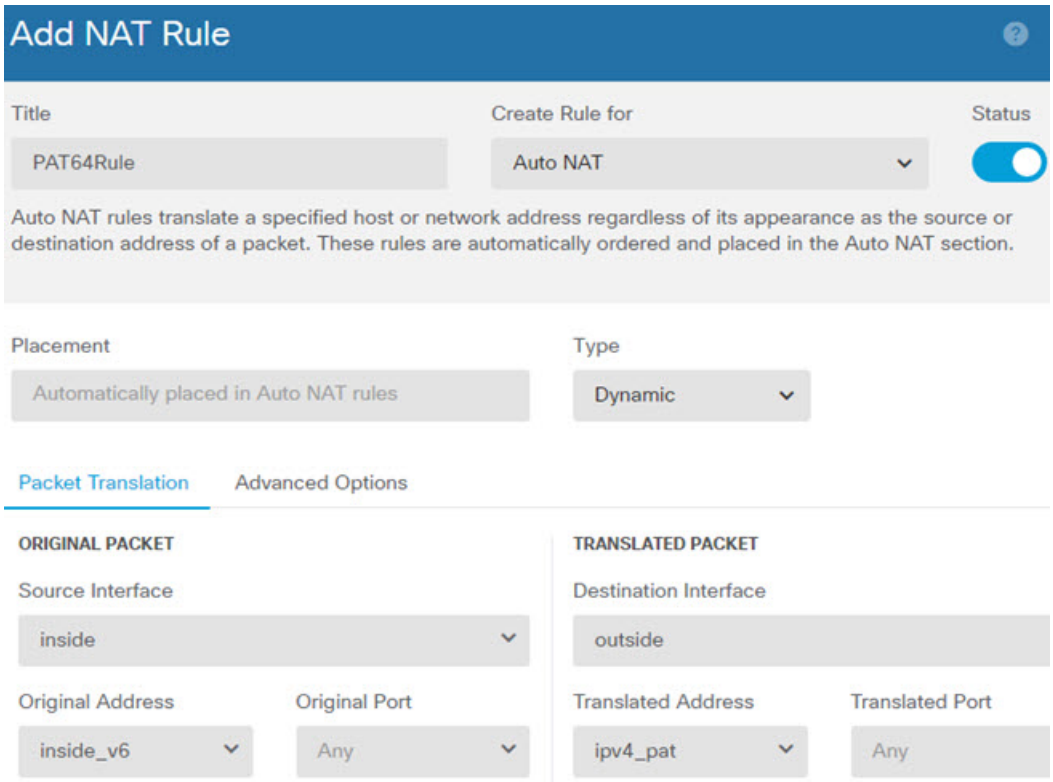


d) Cliquez sur **OK**.

Étape 4 Configurez la règle PAT dynamique pour le réseau IPv6 interne.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton +.
c) Configurez les propriétés suivantes :

- **Titre** = PAT64Rule (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse originale** = inside_v6 network object.
- **Adresse traduite** = ipv4_pat network object.



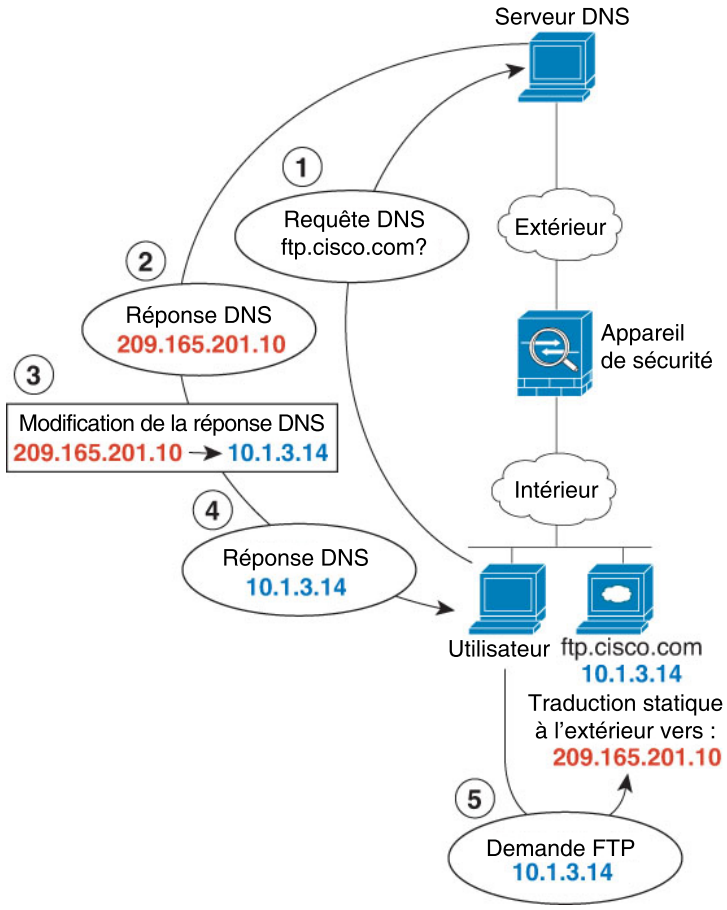
d) Cliquez sur **OK**.

Modification de la réponse DNS, serveur DNS externe

La figure suivante montre un serveur DNS accessible à partir de l'interface externe. Un serveur, ftp.cisco.com, se trouve sur l'interface interne. Vous configurez NAT pour traduire statiquement l'adresse réelle ftp.cisco.com (10.1.3.14) en une adresse mappée (20.165.201.10) visible sur le réseau externe.

Dans ce cas, vous souhaitez activer la modification de la réponse DNS pour cette règle statique afin que les utilisateurs internes qui ont accès à ftp.cisco.com avec l'adresse réelle reçoivent l'adresse réelle du serveur DNS, et non l'adresse mappée.

Lorsqu'un hôte interne envoie une requête DNS pour l'adresse ftp.cisco.com, le serveur DNS répond par l'adresse mappée (209.165.201.10). Le système fait référence à la règle statique pour le serveur interne et traduit l'adresse dans la réponse DNS au format 10.3.1.14. Si vous n'activez pas la modification de la réponse DNS, l'hôte interne tente d'envoyer le trafic vers l'adresse 209.165.201.10 au lieu d'accéder directement à ftp.cisco.com.



Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, vous devez dupliquer les règles pour chaque interface membre.

Procédure

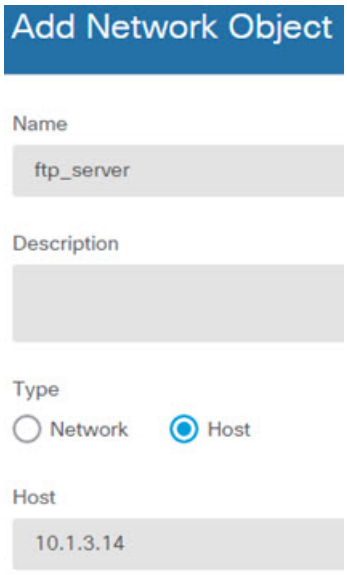
Étape 1 Créez les objets réseau pour le serveur FTP.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.

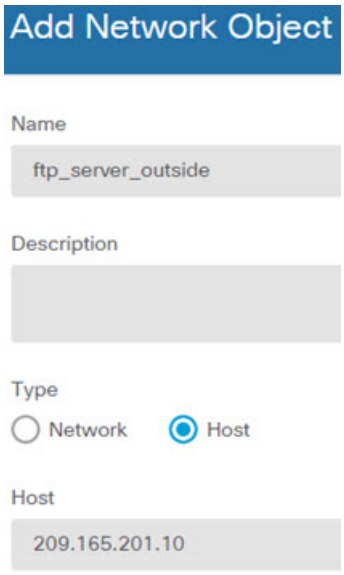
c) Définissez l'adresse réelle du serveur FTP.

Nommez l'objet réseau (par exemple, ftp_server), sélectionnez **Host** (Hôte), et saisissez l'adresse IP réelle de l'hôte, 10.1.3.14.



d) Cliquez sur **OK**.
e) Cliquez sur + et définissez l'adresse traduite du serveur FTP.

Nommez l'objet réseau (par exemple, ftp_server_outside), sélectionnez **Host** (Hôte), puis saisissez l'adresse de l'hôte, 209.165.201.10.

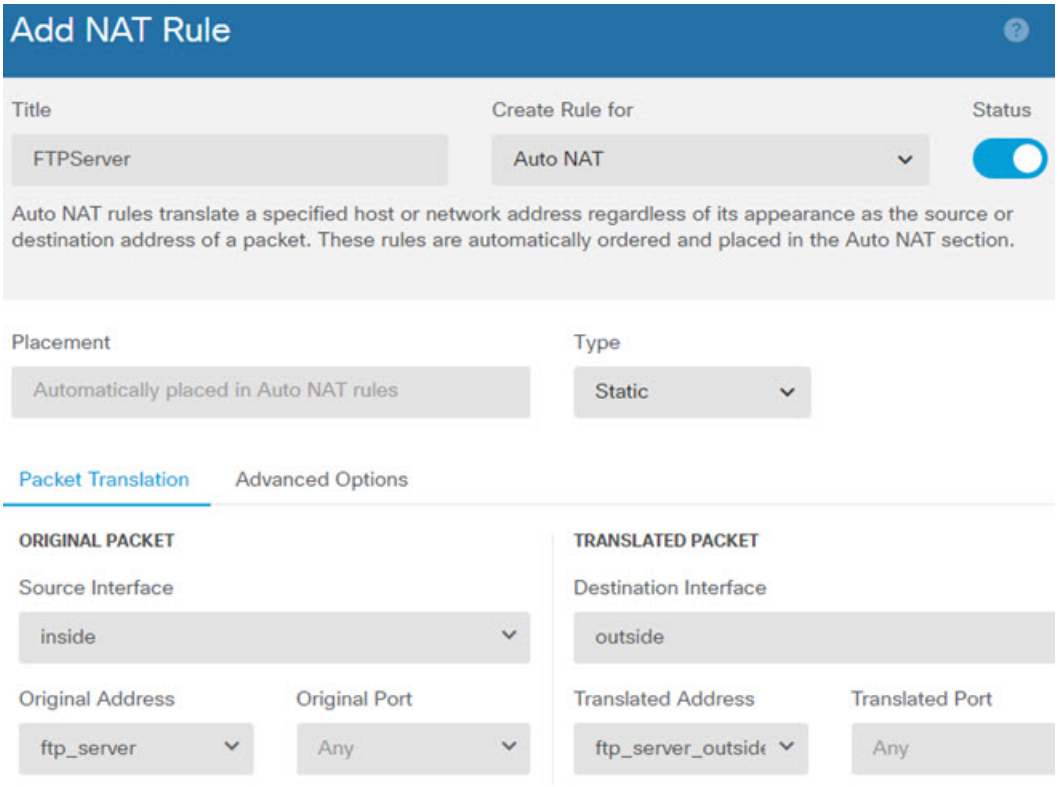


Étape 2 Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton +.
c) Configurez les propriétés suivantes :

- **Titre** = FTPServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.

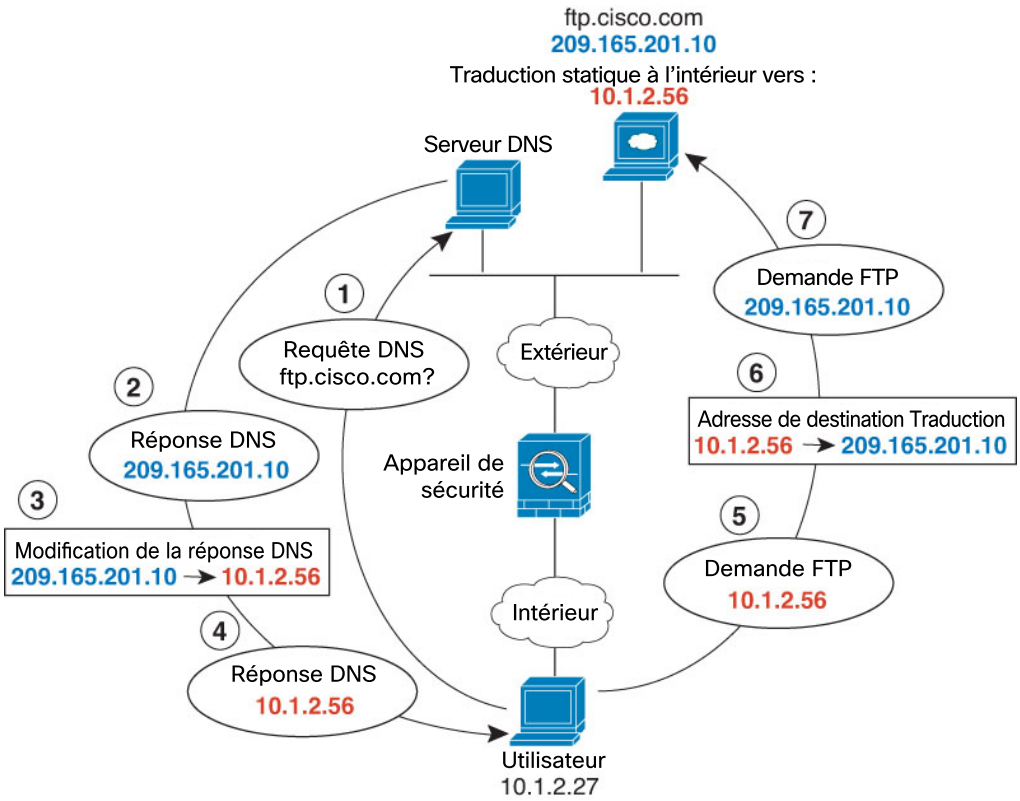
- **Type** = Statique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Original Address (Adresse d'origine)** = objet réseau ftp_server.
- **Translated Address (Adresse traduite)** = objet réseau ftp_server_outside.
- Dans l'onglet **Advanced Options** (Options avancées), sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS correspondant à cette règle).



d) Cliquez sur **OK**.

Modification de la réponse DNS, serveur DNS sur le réseau hôte

La figure suivante montre un serveur FTP et un serveur DNS à l'extérieur. Le système dispose d'une traduction statique pour le serveur externe. Dans ce cas, quand un utilisateur interne demande l'adresse de ftp.cisco.com au serveur DNS, ce dernier répond par l'adresse réelle, 209.165.20.10. Comme vous souhaitez que les utilisateurs internes utilisent l'adresse mappée pour ftp.cisco.com (10.1.2.56), vous devez configurer la modification de la réponse DNS pour la traduction statique.



Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, vous devez dupliquer les règles pour chaque interface membre.

Procédure

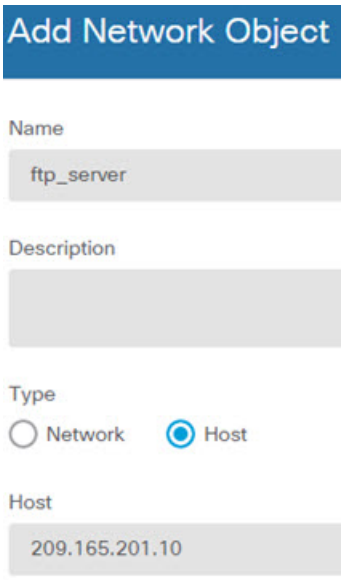
Étape 1 Créez les objets réseau pour le serveur FTP.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur **+**.

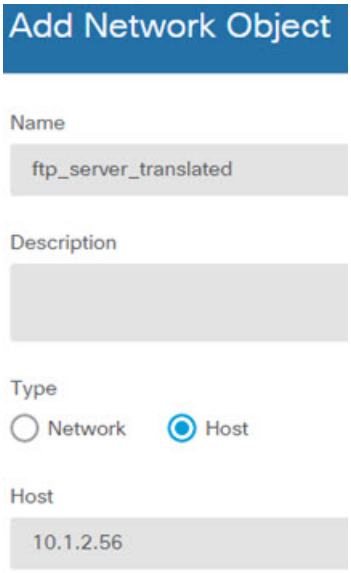
c) Définissez l'adresse réelle du serveur FTP.

Nommez l'objet réseau (par exemple, ftp_server), sélectionnez **Host** (Hôte), et saisissez l'adresse IP réelle de l'hôte, 209.165.201.10.



d) Cliquez sur **OK**.
e) Cliquez sur + et définissez l'adresse traduite du serveur FTP.

Nommez l'objet réseau (par exemple, ftp_server_translated), sélectionnez **Host** (Hôte), et saisissez l'adresse de l'hôte, 10.1.2.56.

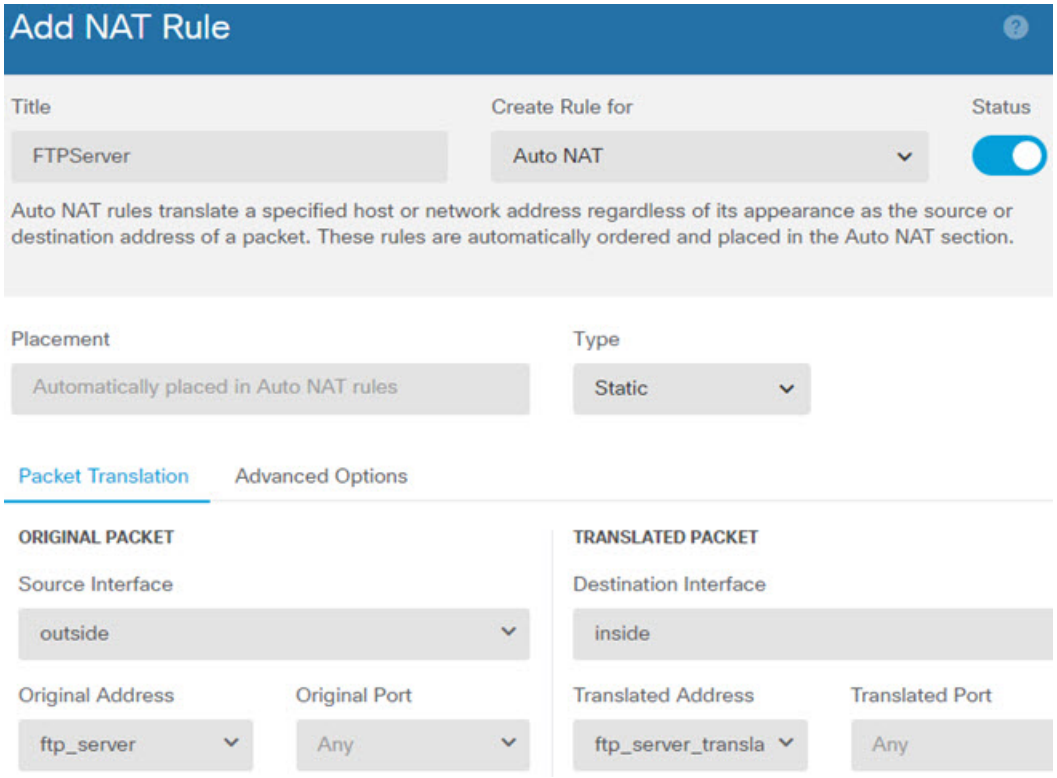


Étape 2 Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton +.
c) Configurez les propriétés suivantes :

- **Titre** = FTPServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.

- **Type** = Statique.
- **Interface source** = externe.
- **Interface de destination** = interne.
- **Adresse d'origine** = objet réseau ftp_server.
- **Adresse traduite** = objet réseau ftp_server_translated.
- Dans l'onglet **Advanced Options** (Options avancées), sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS correspondant à cette règle).



d) Cliquez sur **OK**.



PARTIE VI

Réseaux privés virtuels (VPN)

- VPN de site à site, à la page 659
- VPN d’accès à distance, à la page 703



CHAPITRE 24

VPN de site à site

Un réseau privé virtuel (VPN) est une connexion réseau qui établit un tunnel sécurisé entre des pairs distants en utilisant une source publique, comme Internet ou un autre réseau. Les VPN utilisent des tunnels pour encapsuler les paquets de données dans les paquets IP normaux pour les acheminer sur les réseaux IP. Ils utilisent le chiffrement pour assurer la confidentialité et l'authentification pour assurer l'intégrité des données.

- Principes de base du VPN, à la page 659
- Gestion des VPN de site à site, à la page 667
- Supervision du VPN de site à site, à la page 684
- Exemples de VPN de site à site, à la page 685

Principes de base du VPN

La tunnellisation permet d'utiliser un réseau TCP/IP public, comme Internet, pour créer des connexions sécurisées entre des utilisateurs distants et des réseaux privés d'entreprise. Chaque connexion sécurisée s'appelle un tunnel.

Les technologies VPN basées sur IPsec utilisent les normes de protocole ISAKMP ou IKE (Internet Security Association and Key Management Protocol) et les normes de tunnellisation IPsec pour créer et gérer les tunnels. ISAKMP et IPsec accomplissent les tâches suivantes :

- Négocier les paramètres du tunnel.
- Établir des tunnels.
- Authentifier les utilisateurs et les données.
- Gérer les clés de sécurité.
- Chiffrer et déchiffrer les données.
- Gérer le transfert de données dans le tunnel.
- Gérer le transfert de données entrant et sortant en tant que point terminal de tunnel ou routeur.

Un périphérique dans un VPN fonctionne comme un point terminal de tunnel bidirectionnel. Il peut recevoir des paquets simples du réseau privé, les encapsuler, créer un tunnel 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 du réseau public, les désencapsuler et les envoyer à leur destination finale sur le réseau privé.

Une fois la connexion VPN de site à site établie, les hôtes derrière la passerelle locale peuvent se connecter aux hôtes derrière la passerelle distante par le tunnel VPN sécurisé. Une connexion comprend les adresses IP et les noms d'hôte des deux passerelles, les sous-réseaux derrière elles et la méthode que les deux passerelles utilisent pour s'authentifier l'une auprès de l'autre.

Protocole IKE (Internet Key Exchange)

L'Internet Key Exchange (IKE ou l'échange de clé Internet) est un protocole de gestion de clés utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec.

La négociation IKE comprend deux phases. La phase 1 négocie une association de sécurité entre deux homologues IKE, ce qui permet aux homologues de communiquer de manière sécurisée pendant la phase 2. Pendant la négociation de la phase 2, IKE établit les associations de sécurité pour d'autres applications, telles qu'IPsec. Les deux phases utilisent des propositions lorsqu'elles négocient une connexion.

Une politique IKE est un ensemble d'algorithmes que deux homologues utilisent pour sécuriser la négociation IKE entre eux. La négociation IKE commence lorsque chaque homologue s'accorde sur une politique IKE commune (partagée). Cette politique énonce les paramètres de sécurité qui protègent les négociations IKE ultérieures. Pour IKE version 1 (IKEv1), les politiques IKE contiennent un seul ensemble d'algorithmes et un groupe modulo. Contrairement à IKEv1, dans une politique IKEv2, vous pouvez sélectionner plusieurs algorithmes et groupes de modules parmi lesquels les homologues peuvent choisir pendant la négociation de la phase 1. Il est possible de créer une seule politique IKE, bien que vous puissiez souhaiter que différentes politiques accordent une priorité plus élevée aux options les plus souhaitées. Pour les VPN de site à site, vous pouvez créer une politique IKE.

Pour définir une politique IKE, spécifiez :

- Une priorité unique (de 1 à 65 543, 1 étant la priorité la plus élevée).
- Une méthode de chiffrement pour la négociation IKE, afin de protéger les données et de garantir la confidentialité.
- Une méthode HMAC (hachage de codes d'authentification de message) (appelée algorithme d'intégrité dans IKEv2) pour s'assurer de l'identité de l'expéditeur et pour s'assurer que le message n'a pas été modifié pendant le transfert.
- Pour IKEv2, une fonction pseudo-aléatoire (PRF) distincte est utilisée comme algorithme pour extraire le contenu de la clé et les opérations de hachage nécessaires pour le chiffrement du tunnel IKEv2. Les options sont les mêmes que celles utilisées pour l'algorithme de hachage.
- Un groupe Diffie-Hellman pour déterminer la force de l'algorithme de détermination de la clé de chiffrement. Le périphérique utilise cet algorithme pour déduire les clés de chiffrement et de hachage.
- Une méthode d'authentification pour garantir l'identité des homologues.
- Une limite de temps pendant laquelle le périphérique utilise une clé de chiffrement avant de la remplacer.

Lorsque la négociation IKE commence, l'homologue qui commence la négociation envoie toutes ses politiques activées à l'homologue distant, et l'homologue distant recherche une correspondance avec ses propres politiques, par ordre de priorité. Il existe une correspondance entre les politiques IKE, si elles ont les mêmes valeurs de chiffrement, de hachage (intégrité et PRF pour IKEv2), d'authentification et de Diffie-Hellman, et une durée de vie d'association inférieure ou égale à la durée de vie indiquée dans la politique envoyée. Si les durées de vie ne sont pas identiques, la durée de vie la plus courte, obtenue de l'homologue distant, s'applique. Par défaut, une politique IKE simple qui utilise DES est la seule politique activée. Vous pouvez activer d'autres

politiques IKE avec des priorités plus élevées pour négocier des normes de chiffrement plus strictes, mais la politique DES devrait garantir la réussite de la négociation.

Dans quelle mesure une connexion VPN doit-elle être sécurisée?

Étant donné qu'un tunnel VPN traverse généralement un réseau public, très probablement Internet, vous devez chiffrer la connexion pour protéger le trafic. Vous définissez le chiffrement et les autres techniques de sécurité à appliquer à l'aide des politiques IKE et des propositions IPsec.

Si votre licence vous permet d'appliquer un chiffrement renforcé, vous pouvez choisir parmi un large éventail d'algorithmes de chiffrement et de hachage et de groupes Diffie-Hellman. Cependant, en règle générale, plus le chiffrement que vous appliquez au tunnel est fort, plus les performances du système sont mauvaises. Trouvez un équilibre entre sécurité et performance qui offre une protection suffisante sans compromettre l'efficacité.

Nous ne pouvons pas fournir de conseils précis sur les options à choisir. Si vous agissez au sein d'une grande entreprise ou d'une autre organisation, vous devez peut-être vous conformer à des normes déjà définies. Sinon, prenez le temps d'étudier les options.

Les rubriques suivantes expliquent les options disponibles.

Choix de l'algorithme de chiffrement à utiliser

Au moment de décider quels algorithmes de chiffrement utiliser pour la politique IKE ou la proposition IPsec, votre choix se limite aux algorithmes pris en charge par les périphériques du VPN.

Pour IKEv2, vous pouvez configurer plusieurs algorithmes de chiffrement. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Pour IKEv1, vous ne pouvez sélectionner qu'une seule option.

Pour les propositions IPsec, l'algorithme est utilisé par le protocole ESP (Encapsulating Security Protocol), qui fournit des services d'authentification, de chiffrement et d'anti-relecture. ESP est un protocole IP de type 50. Dans les propositions IKEv1 IPsec, le nom de l'algorithme commence par ESP-.

Si votre licence de périphérique est admissible au chiffrement fort, vous pouvez choisir parmi les algorithmes de chiffrement suivants. Si vous n'êtes pas autorisé à utiliser le cryptage renforcé, vous pouvez sélectionner DES uniquement.



Remarque Si vous êtes qualifié pour un cryptage renforcé, avant de passer de la licence d'évaluation à une licence Smart, vérifiez et mettez à jour vos algorithmes de chiffrement pour un chiffrement plus fort afin que la configuration VPN fonctionne correctement. Choisissez des algorithmes basés sur AES. DES n'est pas pris en charge si vous êtes inscrit avec un compte prenant en charge le cryptage renforcé. Après l'enregistrement, vous ne pouvez pas déployer les modifications avant d'avoir supprimé toutes les utilisations de DES.

- AES-GCM : (IKEv2 uniquement) Le chiffrement avancé standard en mode Galois/compteur est un mode de fonctionnement de chiffrement par bloc qui assure la confidentialité et l'authentification de l'origine des données, et qui offre une sécurité supérieure à l'AES. AES-GCM offre trois forces de clé différentes : les clés de 128, 192 et 256 bits. Une clé plus longue offre une sécurité plus élevée, mais une réduction des performances. GCM est un mode AES nécessaire pour prendre en charge NSA Suite B. NSA Suite B est un ensemble d'algorithmes cryptographiques que les périphériques doivent prendre en charge pour répondre aux normes fédérales en matière de force cryptographique. .

- AES : Advanced Encryption Standard est un algorithme de chiffrement symétrique qui offre une sécurité supérieure à DES et qui est plus efficace que le 3DES du point de vue informatique. AES offre trois puissances de clé différentes : les clés de 128, 192 et 256 bits. Une clé plus longue offre une sécurité plus élevée, mais une réduction des performances.
- DES, la norme de chiffrement des données, qui chiffre à l'aide de clés de 56 bits, est un algorithme de blocage de clé secrète symétrique. Si votre compte de licence ne répond pas aux exigences du contrôle des exportations, ceci est votre seule possibilité.
- Null, ESP-Null – Un algorithme de chiffrement Null permet une authentification sans chiffrement. Cette méthode n'est pas sécurisée ; utilisez-la à votre guise.

Décider des algorithmes de hachage à utiliser

Dans les politiques IKE, l'algorithme de hachage crée un condensé du message, qui est utilisé pour assurer l'intégrité du message. Dans IKEv2, l'algorithme de hachage est séparé en deux options, une pour l'algorithme d'intégrité et une pour la fonction pseudo-aléatoire (PRF).

Dans les propositions IPsec, l'algorithme de hachage est utilisé par le protocole ESP (Encapsulating Security Protocol) pour l'authentification. Dans les propositions IKEv2 IPsec, cela s'appelle le hachage d'intégrité. Dans les propositions IKEv1 IPsec, le nom de l'algorithme est précédé de ESP-, et il y a également un suffixe -HMAC (qui signifie « code d'authentification de la méthode de hachage »).

Pour IKEv2, vous pouvez configurer plusieurs algorithmes de hachage. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Pour IKEv1, vous ne pouvez sélectionner qu'une seule option.

Vous pouvez choisir parmi les algorithmes de hachage suivants.

- SHA (Secure Hash Algorithm) : la norme SHA (SHA1) produit un condensé de 160 bits.

  Les options SHA-2 suivantes, qui sont encore plus sécurisées, sont disponibles pour les configurations IKEv2. Choisissez l'une de ces spécifications si vous souhaitez mettre en œuvre la spécification de chiffrement de la suite B de NSA.

  - SHA256 : spécifie l'algorithme de hachage sécurisé SHA2 avec le condensé 256 bits.
  - SHA384 : spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 384 bits.
  - SHA512 : spécifie l'algorithme Secure Hash SHA2 avec le condensé 512 bits.

- Null ou aucun (NULL, ESP-NONE) : (propositions IPsec uniquement.) un algorithme de hachage nul; cela est généralement utilisé à des fins de test uniquement. Cependant, vous devez choisir l'algorithme d'intégrité nulle si vous sélectionnez l'une des options AES-GCM comme algorithme de chiffrement. Même si vous choisissez une option non nulle, le hachage d'intégrité est ignoré pour ces normes de chiffrement.

Choix du groupe de module Diffie-Hellman à utiliser

Vous pouvez utiliser les algorithmes de dérivation de clé Diffie-Hellman suivants pour générer des clés d'association de sécurité IPsec. Chaque groupe a un module de taille différent. Un module plus élevé offre une sécurité élevée, mais nécessite plus de temps de traitement. Vous devez avoir un groupe de module correspondant sur les deux homologues.

Si vous sélectionnez le chiffrement AES, pour prendre en charge les grandes tailles de clés requises par AES, vous devez utiliser le groupe Diffie-Hellman (DH) 5 ou supérieur. Les politiques IKEv1 ne prennent pas en charge tous les groupes répertoriés ci-dessous.

Pour mettre en œuvre la spécification de Chiffrement B de NSA, utilisez IKEv2 et sélectionnez l'une des options ECDH (elliptique courbe Diffie-Hellman) : 19, 20 ou 21. Les options de courbe elliptique et les groupes qui utilisent un module de 2048 bits sont moins exposés aux attaques telles que Logjam.

Pour IKEv2, vous pouvez configurer plusieurs groupes. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Pour IKEv1, vous ne pouvez sélectionner qu'une seule option.

- 14 : Groupe Diffie-Hellman 14 : groupe MODP (exponentiel modulaire) 2048 bits. Considérées comme une bonne protection pour les clés de 192 bits.
- 15 : Groupe Diffie-Hellman 15 : groupe MODP 3 072 bits.
- 16 : Groupe Diffie-Hellman 16 : groupe MODP 4096 bits.
- 19 : Groupe Diffie-Hellman 19 : Courbe elliptique 256 bits modulo un nombre premier (ECP) du National Institue of Standards and Technology (NIST).
- 20 : Groupe Diffie-Hellman 20 : Groupe ECP NIST 384 bits.
- 21 : Groupe Diffie-Hellman 21 : Groupe ECP NIST 521 bits.
- 31 : Groupe Diffie-Hellman 31 : Courbe 25519 256 bits, groupe EC.

Choix de la méthode d'authentification à utiliser

Vous pouvez utiliser les méthodes suivantes pour authentifier les homologues dans une connexion VPN de site à site.

Clés prépartagées

Les clés prépartagées sont des chaînes de clés secrètes configurées sur chaque homologue de la connexion. Ces clés sont utilisées par IKE pendant la phase d'authentification. Pour IKEv1, vous devez configurer la même clé prépartagée sur chaque homologue. Pour IKEv2, vous pouvez configurer des clés uniques sur chaque homologue.

Les clés prépartagées ne sont pas aussi évolutives que les certificats. Si vous devez configurer un grand nombre de connexions VPN de site à site, utilisez la méthode des certificats plutôt que la méthode de la clé prépartagée.

Certificats

Les certificats numériques utilisent des paires de clés RSA pour signer et chiffrer les messages de gestion des clés IKE. Lorsque vous configurez chaque extrémité de la connexion VPN site-à-site, vous sélectionnez le certificat d'identité du périphérique local, afin que l'homologue distant puisse authentifier l'homologue local.

Pour utiliser la méthode du certificat, vous devez effectuer les opérations suivantes :

1. Enregistrez votre homologue local auprès d'une autorité de certification (CA) et obtenez un certificat d'identité d'appareil. Chargez ce certificat sur le périphérique. Pour en savoir plus, consultez Charger les certificats d'identité interne et d'autorité de certification interne, à la page 161.

Si vous êtes également responsable de l'homologue distant, enregistrez également cet homologue. Bien qu'il soit pratique d'utiliser la même autorité de certification pour les homologues, il n'est pas obligatoire.

Vous ne pouvez pas utiliser un certificat autosigné pour établir une connexion VPN. Vous devez inscrire le périphérique auprès d'une autorité de certification.

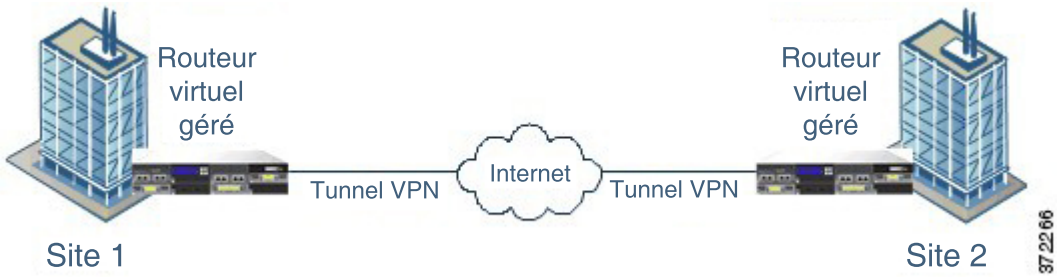
Si vous utilisez une autorité de certification Windows pour créer des certificats pour les points terminaux VPN de site à site, vous devez utiliser un certificat qui spécifie le système terminal de sécurité IP pour l'extension des politiques d'application. Vous pouvez le trouver dans la boîte de dialogue des propriétés du certificat, sous l'onglet Extensions (sur le serveur Windows CA). La valeur par défaut pour cette extension est IP security IKE intermédiaire, qui ne fonctionne pas pour un VPN de site à site configuré à l'aide de Gestionnaire de périphériques de pare-feu.

2. Chargez le certificat d'autorité de certification de confiance qui a été utilisé pour signer le certificat d'identité de l'homologue local. Si vous avez utilisé une autorité de certification intermédiaire, chargez la chaîne complète, y compris les certificats racine et intermédiaire. Pour en savoir plus, consultez Téléchargement des certificats de l'autorité de certification de confiance, à la page 165.
3. Si l'homologue distant était inscrit auprès d'une autorité de certification différente, chargez également le certificat d'autorité de certification de confiance utilisé pour signer le certificat d'identité de l'homologue distant. Obtenez le certificat de l'organisation qui contrôle l'homologue distant. S'ils ont utilisé une autorité de certification intermédiaire, chargez la chaîne complète, y compris les certificats racine et intermédiaire.
4. Lorsque vous configurez la connexion VPN de site à site, sélectionnez la méthode de certificat, puis sélectionnez le certificat d'identité de l'homologue local. Chaque extrémité de la connexion spécifie le certificat pour l'extrémité locale de la connexion; vous ne spécifiez pas le certificat pour l'homologue distant.

Topologies VPN

Vous pouvez configurer uniquement les connexions VPN point à point en utilisant Gestionnaire de périphériques de pare-feu. Bien que toutes les connexions soient point à point, vous pouvez vous connecter à des VPN plus importants en étoile ou en maillage en définissant chacun des tunnels auxquels votre périphérique participe.

Le diagramme suivant présente une topologie VPN point à point typique. Dans une topologie VPN point à point, deux points terminaux communiquent directement l'un avec l'autre. Vous configurez les deux points terminaux en tant qu'périphériques homologues, et l'un ou l'autre des périphériques peut démarrer la connexion sécurisée.



Établissement de connexions VPN de site à site avec des homologues à adresse dynamique

Vous pouvez créer des connexions VPN de site à site avec des homologues même lorsque vous ne connaissez pas l'adresse IP de l'homologue. Cela peut être utile dans les situations suivantes :

- Si l'homologue obtient son adresse à l'aide de DHCP, vous ne pouvez pas dépendre du point terminal distant d'une adresse IP statique spécifique.
- Lorsque vous souhaitez autoriser un nombre indéterminé d'homologues distants à établir une connexion avec le périphérique, qui servira de concentrateur dans une topologie en étoile.

Lorsque vous devez établir une connexion sécurisée avec un homologue B dont l'adresse est attribuée dynamiquement, vous devez vous assurer que l'extrémité de la connexion, A, dispose d'une adresse IP statique. Ensuite, lorsque vous créez la connexion sur A, spécifiez que l'adresse de l'homologue est dynamique. Toutefois, lorsque vous configurez la connexion sur l'homologue B, veillez à saisir l'adresse IP de A comme adresse d'homologue distant.

Lorsque le système établit des connexions VPN de site à site, toutes les connexions pour lesquelles l'homologue possède une adresse dynamique seront de réponse uniquement. C'est-à-dire que l'homologue distant doit être celui qui amorce la connexion. Lorsque l'homologue distant tente d'établir la connexion, votre périphérique valide la connexion à l'aide de la clé prépartagée ou du certificat, selon la méthode que vous avez définie dans la connexion.

Étant donné que la connexion VPN est établie uniquement après que l'homologue distant a lancé la connexion, tout trafic sortant correspondant aux règles de contrôle d'accès qui autorisent le trafic dans le tunnel VPN sera abandonné jusqu'à ce que cette connexion soit établie. Cela garantit que les données ne quittent pas votre réseau sans le chiffrement et la protection VPN appropriés.

Virtual Tunnel Interfaces et VPN basé sur le routage

Traditionnellement, vous configurez une connexion VPN de site à site en définissant les réseaux locaux et distants spécifiques qui seront chiffrés sur le tunnel VPN. Ceux-ci sont définis dans une carte cryptographique qui fait partie du profil de connexion VPN. Ce type de VPN de site à site est appelé basé sur les politiques.

Vous pouvez également configurer un VPN de site à site basé sur le routage. Dans ce cas, vous créez une interface de tunnel virtuel (VTI), qui est une interface virtuelle associée à une interface physique spécifique, généralement l'interface externe. Ensuite, vous utilisez la table de routage, avec des routes statiques et dynamiques, pour diriger le trafic souhaité vers le VTI. Tout trafic acheminé par le VTI (sortant) est chiffré sur le tunnel VPN que vous configurez pour le VTI.

Avec le VPN de site à site basé sur le routage, vous gérez les réseaux protégés dans une connexion VPN donnée en modifiant simplement la table de routage, sans modifier le profil de la connexion VPN. Vous n'avez pas besoin de suivre les réseaux distants et de mettre à jour le profil de connexion VPN pour prendre en compte ces modifications. Cela simplifie la gestion du VPN pour les fournisseurs de services infonuagiques et les grandes entreprises.

En outre, vous pouvez créer des règles de contrôle d'accès pour le VTI afin d'affiner les types de trafic autorisés dans le tunnel. Par exemple, vous pouvez appliquer l'inspection de prévention des intrusions et le filtrage des URL et des applications.

Aperçu du processus de configuration des VPN basés sur le routage

En tant qu'aperçu, le processus de configuration d'un VPN de site à site basé sur le routage comprend les étapes suivantes :

Procédure

Étape 1 Créez la politique IKEv1/2 et la proposition IPsec pour le terminal local.

Étape 2 Créez une interface de tunnel virtuel (VTI) associée à l'interface physique qui fait face à l'homologue distant.

Étape 3 Créez le profil de connexion VPN de site à site qui utilise le VTI, la politique IKE et la proposition IPsec.

Étape 4 Créez les mêmes propositions IKE et IPsec sur l'homologue distant, et un VTI distant, et le profil de connexion VPN de site à site qui spécifie ce VTI local comme point terminal distant (du point de vue de l'homologue distant).

Étape 5 Créez des routes et des règles de contrôle d'accès sur les deux homologues pour envoyer le trafic approprié dans le tunnel.

Assurez-vous que les routes et le contrôle d'accès sur chaque terminal sont en miroir, pour permettre au trafic de circuler dans les deux sens.

Les routes statiques auraient ces caractéristiques générales :

- **Interface** : nom de l'interface de tunnel virtuel (VTI).
- **Networks**(réseaux) : objets réseau qui définissent les réseaux distants protégés par le terminal distant.
- **Gateway** (Passerelle) : objet réseau qui définit l'adresse IP du point terminal distant du tunnel VPN.

Lignes directrices pour les interfaces de tunnel virtuel et VPN basé sur le routage

Directives IPv6

Les interfaces de tunnel virtuel prennent uniquement en charge les adresses IPv4. Vous ne pouvez pas configurer une adresse IPv6 sur un VTI.

Directives supplémentaires

- Vous pouvez créer un maximum de 1 024 VTI.
- Vous ne pouvez pas configurer l'injection de route inverse, statique ou dynamique, sur un VPN basé sur le routage VTI. (Vous pouvez configurer l'injection de route inverse à l'aide de l'API Firewall Threat Defense uniquement.)
- Vous ne pouvez pas configurer une adresse d'homologue dynamique lorsque vous sélectionnez un VTI comme interface locale.
- Vous ne pouvez pas configurer d'homologues de sauvegarde à distance lorsque vous sélectionnez un VTI comme interface locale.

- Vous ne pouvez pas créer de VTI pour une interface source qui est affectée à un routeur virtuel personnalisé. Lorsque vous utilisez des routeurs virtuels, vous pouvez configurer des VTI sur les interfaces du routeur virtuel global uniquement.
- Les associations de sécurité IKE et IPsec seront rachetées en permanence, quel que soit le trafic de données dans le tunnel. Cela garantit que les tunnels VTI sont toujours actifs.
- Vous ne pouvez pas configurer à la fois IKEv1 et IKEv2 sur un profil de connexion basé sur le routage : vous ne devez configurer qu'une seule version IKE.
- Les configurations du VTI et de la carte de chiffrement peuvent coexister sur la même interface physique, à condition que l'adresse homologue configurée dans la carte de chiffrement et la destination du tunnel pour le VTI soient différentes.
- Seul le protocole de routage BGP est pris en charge sur le VTI.
- Si le système met fin aux clients IKEv2 VTI IOS, désactivez la demande config-exchange sur IOS, car le système ne peut pas récupérer les attributs mode-CFG pour la session initiée par un client VTI IOS.
- Les VPN de site à site basés sur le routage sont configurés comme bidirectionnels, ce qui signifie que l'un ou l'autre des points terminaux du tunnel VPN peut lancer la connexion. Après avoir créé le profil de connexion, vous pouvez modifier ce point terminal pour qu'il soit soit le seul initiateur (INITIATE_ONLY) ou exclusivement le répondeur (RESPOND_ONLY). Assurez-vous de modifier le terminal distant pour utiliser le type de connexion complémentaire. Pour apporter cette modification, vous devez accéder à l'explorateur d'API et utiliser GET /devices/default/s2sconnectionprofiles pour trouver le profil de connexion. Vous pouvez ensuite copier/coller le contenu du corps dans la méthode PUT /devices/default/s2sconnectionprofiles/{objId}, mettre à jour **connectionType** pour préciser le type souhaité et exécuter la méthode.

Gestion des VPN de site à site

Un réseau privé virtuel (VPN) est une connexion réseau qui établit un tunnel sécurisé entre des pairs distants en utilisant une source publique, comme Internet ou un autre réseau. Les VPN utilisent des tunnels pour encapsuler les paquets de données dans les paquets IP normaux pour les acheminer sur les réseaux IP. Ils utilisent le chiffrement pour assurer la confidentialité et l'authentification pour assurer l'intégrité des données.

Vous pouvez créer des connexions VPN avec des périphériques homologues. Toutes les connexions sont point à point, mais vous pouvez lier le périphérique à des VPN plus importants en étoile ou maillés en configurant toutes les connexions pertinentes.

Avant de commencer

Les éléments suivants déterminent le type et le nombre de connexions VPN de site à site que vous pouvez recréer :

- Les connexions VPN utilisent le chiffrement pour sécuriser la confidentialité du réseau. Les algorithmes de chiffrement que vous pouvez utiliser varient selon que votre licence de base autorise le chiffrement renforcé. Ceci est contrôlé par le fait que vous ayez sélectionné l'option d'autoriser les fonctionnalités d'exportation contrôlée sur l'appareil lorsque vous vous êtes enregistré auprès du gestionnaire de licences Smart Cisco. Si vous utilisez la licence d'évaluation, ou si vous n'avez pas activé la fonctionnalité contrôlée à l'exportation, vous ne pouvez pas utiliser le cryptage renforcé.

- Vous ne pouvez pas créer plus de 20 profils IPsec uniques. Le caractère unique est déterminé par la combinaison des propositions et des certificats IKEv1/v2, du type de connexion et du groupe DH et de la durée de vie SA. Vous pouvez réutiliser les profils existants. Ainsi, si vous utilisez les mêmes paramètres pour toutes vos connexions VPN de site à site, vous avez un profil IPsec unique. Une fois que vous avez atteint la limite de 20 profils IPsec uniques, vous ne pouvez pas créer de nouvelles connexions VPN de site à site, sauf si vous utilisez la même combinaison d'attributs que vous avez utilisée pour un profil de connexion existant.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis cliquez sur **View Configuration** (Afficher la configuration) dans le groupe VPN de site à site.

Cela ouvre la page VPN de site à site, qui répertorie toutes les connexions que vous avez configurées.

Étape 2 Effectuez l'une des actions suivantes.

- Pour créer une nouvelle connexion VPN de site à site, cliquez sur le bouton +. Consultez Configuration d'une connexion VPN de site à site, à la page 668.

  S'il n'y a aucune connexion pour le moment, vous pouvez également cliquer sur le bouton **Create Site-to-Site Connection** (Créer une connexion de site à site .

- Pour modifier une connexion existante, cliquez sur l'icône de modification ( ) de la connexion. Consultez Configuration d'une connexion VPN de site à site, à la page 668.

- Pour copier un résumé de la configuration de la connexion dans le presse-papier, cliquez sur l'icône de copie ( ) de la connexion. Vous pouvez coller ces informations dans un document et l'envoyer à l'administrateur du périphérique distant pour l'aider à configurer l'autre extrémité de la connexion.

- Pour supprimer une connexion dont vous n'avez plus besoin, cliquez sur l'icône de suppression ( ) de la connexion.

Configuration d'une connexion VPN de site à site

Vous pouvez créer une connexion VPN point à point pour lier votre périphérique à un autre périphérique, en supposant que vous ayez la collaboration et l'autorisation du propriétaire du périphérique distant. Bien que toutes les connexions soient point à point, vous pouvez vous connecter à des VPN plus importants en étoile ou en maillage en définissant chacun des tunnels auxquels votre périphérique participe.

Avant de commencer

Vous pouvez créer une seule connexion VPN par combinaison réseau local/réseau distant. Cependant, vous pouvez créer plusieurs connexions pour un réseau local si le réseau distant est unique dans chaque profil de connexion.

Si les réseaux distants se chevauchent, veillez à créer d'abord le profil de connexion le plus restreint. Le système créera les tunnels dans l'ordre dans lequel vous créez les profils de connexion, et non dans l'ordre dans lequel ils sont affichés (qui est simplement alphabétique).

Par exemple, si vous souhaitez qu'un tunnel de 192.16.0.0/16 à 10.91.0.0/16 aille au point de terminaison distant A, mais que le tunnel 192.16.0.0/24 vers le reste de 10.0.0.0/8 passe par le point de terminaison distant B, vous devez créer le profil de connexion pour A avant de créer celui pour B.

Remarque Si vous créez plusieurs connexions VPN de site à site basées sur des politiques, vous devez spécifier la même interface que l'interface d'accès au VPN local dans chaque profil. Vous ne pouvez pas créer de VPN de site à site basés sur des politiques vers plus d'une interface à l'aide de FDM.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration (Afficher la configuration)** dans le groupe VPN de site à site.

Étape 2 Effectuez l'une des actions suivantes :

- Pour créer une nouvelle connexion VPN de site à site, cliquez sur le bouton **+**.

  S'il n'y a aucune connexion pour le moment, vous pouvez également cliquer sur le bouton **Create Site-to-Site Connection** (Créer une connexion de site à site .

- Pour modifier une connexion existante, cliquez sur l'icône de modification ( ) de la connexion.

Pour supprimer une connexion dont vous n'avez plus besoin, cliquez sur l'icône de suppression ( ) de la connexion.

Étape 3 Définissez les points terminaux de la connexion VPN point à point.

- **Nom du profil de connexion** : le nom de cette connexion, jusqu'à 64 caractères sans espaces. Par exemple, MainOffice. Vous ne pouvez pas utiliser une adresse IP comme nom.
- **Type** : comment vous identifierez le trafic qui doit être envoyé par le tunnel VPN. Sélectionnez l'une des options suivantes :
  - **Basé sur le routage (VTI)** : vous utiliserez la table de routage, principalement les routes statiques, pour définir les réseaux locaux et distants qui doivent participer au tunnel. Si vous sélectionnez cette option, vous devez sélectionner une interface de tunnel virtuel (VTI) comme interface d'accès au VPN local. Vous devez également utiliser une adresse IP statique pour l'extrémité distante du tunnel. Assurez-vous de configurer les routes statiques et les règles de contrôle d'accès appropriées pour le VTI après avoir créé le profil de connexion VPN.
  - **Basé sur les politiques** : vous préciserez les réseaux locaux et distants directement dans le profil de connexion VPN de site à site. Il s'agit de l'approche classique pour définir le trafic qui doit être protégé par le tunnel VPN.
- **Site local** : ces options définissent le point terminal local.

- **Interface d'accès VPN locale** : sélectionnez l'interface à laquelle l'homologue distant peut se connecter. Il s'agit généralement de l'interface externe. L'interface ne peut pas faire partie d'un groupe de pont.
- **Réseau local** :(basé sur les politiques uniquement) Cliquez + et sélectionnez les objets réseau qui identifient les réseaux locaux qui doivent participer à la connexion VPN. Les utilisateurs de ces réseaux pourront atteindre les réseaux distants par la connexion.

Remarque
Vous pouvez utiliser des adresses IPv4 ou IPv6 pour ces réseaux, mais vous devez avoir un type d'adresse correspondant de chaque côté de la connexion. Par exemple, la connexion VPN pour un réseau IPv4 local doit avoir au moins un réseau IPv4 distant. Vous pouvez combiner IPv4 et IPv6 des deux côtés d'une connexion unique. Les réseaux protégés pour les points terminaux ne peuvent pas se chevaucher.

- **Site distant** : ces options définissent le terminal distant.
  - **Static**(Statique)/**Dynamic**(Dynamique) : si l'adresse IP de l'homologue distant est définie de manière statique ou dynamique (par exemple, par DHCP). Si vous sélectionnez **Static** (Statique), saisissez également l'adresse IP de l'homologue distant. Si vous sélectionnez **Dynamic** (Dynamique), seul l'homologue distant pourra établir cette connexion VPN.

    Pour le VPN basé sur le routage, vous pouvez sélectionner **Static** (Statique) uniquement.
  - **Adresse IP distante** (adressage statique uniquement.) : Saisissez l'adresse IP de l'interface de l'homologue du VPN distant qui accueillera la connexion VPN.
  - **Réseau distant** :(basé sur les politiques uniquement) Cliquez + et sélectionnez les objets réseau qui identifient les réseaux distants qui doivent participer à la connexion VPN. Les utilisateurs de ces réseaux pourront atteindre les réseaux locaux par le biais de la connexion.

Étape 4 Cliquez sur **Next** (suivant).

Étape 5 Définissez la configuration de confidentialité pour le VPN.

Remarque
Votre licence détermine les protocoles de chiffrement que vous pouvez sélectionner. Vous devez être admissible au chiffrement renforcé, c'est-à-dire satisfaire aux contrôles des exportations, pour pouvoir choisir d'autres options que les plus basiques.ions, pour choisir tout, sauf les options les plus simples.

- **Version IKE 2**, **Version IKE 1** : choisissez les versions IKE à utiliser lors des négociations d'Internet Key Exchange (IKE). Pour les connexions basées sur des politiques, vous pouvez sélectionner l'une ou les deux; pour celles basées sur le routage, vous ne pouvez sélectionner qu'une seule. Lorsque le périphérique tente de négocier une connexion avec l'autre homologue, il utilise les versions que vous autorisez et que l'autre homologue accepte. Si vous autorisez les deux versions, le périphérique revient automatiquement à l'autre version si les négociations échouent avec la version initialement choisie. IKEv2 est toujours essayé en premier s'il est configuré. Les deux homologues doivent prendre en charge IKEv2 pour l'utiliser dans une négociation.
- **Politique IKE** : Internet Key Exchange (IKE) est un protocole de gestion de clés utilisé pour authentifier les homologues IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec (SA). Il s'agit d'une politique globale : les objets que vous activez sont appliqués à tous les VPN. Cliquez sur **Edit** (Modifier) pour examiner les politiques actuellement activées globalement par version IKE, puis pour activer et créer de nouvelles politiques. Pour en savoir plus, consultez Configuration de la politique IKE globale, à la page 674.

- **Proposition IPsec** : la proposition IPsec définit la combinaison de protocoles et d'algorithmes de sécurité qui sécurisent le trafic dans un tunnel IPsec. Cliquez sur **Edit** (Modifier) et sélectionnez les propositions pour chaque version IKE. Sélectionnez toutes les propositions que vous souhaitez autoriser. Cliquez sur **Set Default** (Définir par défaut) pour simplement sélectionner les valeurs par défaut du système, qui varient en fonction de votre conformité aux règles d'exportation. Le système négocie avec l'homologue, en commençant par le groupe le plus fort vers le plus faible jusqu'à ce qu'une correspondance soit trouvée. Pour en savoir plus, consultez Configuration des propositions IPsec, à la page 679.
- **Authentication Type** (type d'authentification) : comment vous souhaitez authentifier les homologues dans la connexion VPN, soit **par clé manuelle prépartagée**, soit **par certificat**. Vous devez également remplir les champs suivants en fonction de votre sélection. Pour IKEv1, votre sélection doit correspondre à la méthode d'authentification sélectionnée dans l'objet de politique IKEv1 configuré pour la connexion. Pour des informations détaillées sur les options, consultez Choix de la méthode d'authentification à utiliser, à la page 663.
  - (IKEv2) **Local Preshared Key** (Clé prépartagée locale), **Remote Peer Preshared Key** (Clé prépartagée d'homologue distant) : les clés définies sur ce périphérique et sur le périphérique distant pour la connexion VPN. Ces clés peuvent être différentes dans IKEv2. La clé peut comporter entre 1 et 127 caractères alphanumériques.
  - (IKEv1) **Clé prépartagée** : la clé qui est définie sur les périphériques locaux et distants. La clé peut comporter entre 1 et 127 caractères alphanumériques.
  - **Certificate** (Certificat) : le certificat d'identité du périphérique pour l'homologue local. Il doit s'agir d'un certificat obtenu auprès d'une autorité de certification (CA) ; vous ne pouvez pas utiliser de certificat autosigné. Si vous n'avez pas chargé le certificat, cliquez sur le lien **Create New Object** (Créer un nouvel objet). Vous devez également télécharger le certificat racine et tous les certificats d'autorité de certification intermédiaires de confiance utilisés pour signer le certificat d'identité. Si vous ne les avez pas encore chargés, vous pouvez le faire après avoir terminé cet assistant.
- **IPsec Settings** (Paramètres IPsec) : la durée de vie de l'association de sécurité. Une fois la durée de vie atteinte, le système renégocie l'association de sécurité. Lorsque le système reçoit une demande de négociation de l'homologue, il utilise la plus petite des durées de vie proposées par l'homologue ou configurées localement comme durée de vie des nouvelles associations de sécurité. Il existe deux durées de vie : une durée de vie « temporelle » et une durée de vie « en fonction du volume de trafic ». L'association de sécurité expire lorsque la première de ces deux durées de vie est atteinte.
  - **Lifetime Duration** (Durée de vie) : le nombre de secondes pendant lesquelles une association de sécurité peut rester active avant d'expirer. La plage est comprise entre 120 et 214783647 secondes. La valeur globale par défaut est de 28 800 secondes (huit heures).
  - **Lifetime Size** (Taille de durée de vie) : le volume de trafic (en kilo-octets) qui peut passer entre les homologues à l'aide d'une association de sécurité donnée avant son expiration. La plage est de 10 à 2147483647 kilo-octets, ou le champ est vide. La valeur par défaut est de 4 608 000 kilo-octets. Laissez le champ vide pour supprimer la limite basée sur la taille et utiliser uniquement la durée comme limite.
- **NAT Exempt**(exemption de NAT) :(basé sur les politiques uniquement) Indique s'il faut exempter le trafic VPN des politiques de NAT sur l'interface d'accès VPN locale. Si vous ne souhaitez pas que les règles NAT s'appliquent au réseau local, sélectionnez l'interface qui héberge le réseau local. Cette option ne fonctionne que si le réseau local se trouve derrière une interface de routage unique (et non un membre d'un groupe de ponts). Si le réseau local se trouve derrière plusieurs interfaces de routage ou un ou plusieurs membres de groupes de pont, vous devez créer manuellement les règles d'exemption NAT.

Pour plus d'informations sur la création manuelle des règles requises, consultez Exemption du trafic VPN de site à site de la NAT, à la page 685.

- **Diffie-Hellman Group for Perfect Forward Secrecy** (Groupe Diffie-Hellman pour la confidentialité de transmission parfaite) : indique s'il faut utiliser la Confidentialité de transmission parfaite (PFS) pour générer et utiliser une clé de session unique pour chaque échange chiffré. La clé de session unique protège l'échange du déchiffrement ultérieur, même si l'échange en entier a été enregistré et que l'agresseur a obtenu les clés prépartagées ou privées utilisées par les terminaux. Pour activer la Confidentialité de transmission parfaite, sélectionnez l'algorithme de dérivation de clé Diffie-Hellman à utiliser pour générer la clé de session PFS dans la liste Modulus Group (groupe de module). Si vous activez IKEv1 et IKEv2, les options sont limitées à celles qu'IKEv1 prend en charge. Pour obtenir une explication des options, consultez Choix du groupe de module Diffie-Hellman à utiliser, à la page 662.

Étape 6 Cliquez sur **Next** (suivant).

Étape 7 Passez en revue le résumé et cliquez sur **Finish** (Terminer).

Les renseignements récapitulatifs sont copiés dans le presse-papiers. Vous pouvez coller ces renseignements dans un document et les utiliser pour vous aider à configurer l'homologue distant ou les envoyer à la personne responsable de la configuration de cet homologue.

Vous devez effectuer des étapes supplémentaires pour autoriser le trafic dans le tunnel VPN, comme expliqué dans Autoriser le trafic via le VPN de site à site, à la page 673.

Après avoir déployé la configuration, connectez-vous à la console d'interface en ligne de commande du périphérique et utilisez la commande **show ipsec sa** pour vérifier que les points terminaux établissent une association de sécurité. Consultez Vérification des connexions VPN de site à site, à la page 681.

Configuration d'une interface de tunnel virtuel

Vous pouvez utiliser une Virtual Tunnel Interface (Interface de tunnel virtuel) (VTI) uniquement dans un profil de connexion VPN de site à site basé sur le routage. Une VTI est associée à une interface physique, par laquelle la connexion VPN est établie avec l'homologue distant. En utilisant une interface virtuelle, vous pouvez simplifier la connexion VPN site à site et contrôler le trafic à l'aide de routes statiques et dynamiques, plutôt que de préciser les réseaux locaux et distants du VPN dans le profil de connexion.

Procédure

Étape 1 Cliquez sur **Device**(Périphérique), cliquez sur le lien dans le résumé des **Interfaces**, puis cliquez sur Virtual Tunnel Interfaces (Interfaces de tunnel virtuel).

Étape 2 Effectuez l'une des actions suivantes :

- Cliquez sur **+** ou sur **Create Virtual Tunnel Interface (Créer une interface de tunnel virtuel)** pour créer une nouvelle interface.
- Cliquez sur l'icône de modification ( ) pour une interface existante.

Si vous n'avez plus besoin d'une interface, cliquez sur l'icône de suppression ( ) pour la supprimer. Vous devez d'abord supprimer tout profil de connexion site à site qui utilise l'interface, avant de pouvoir la supprimer.

Étape 3 Configurez les options suivantes :

- **Name** (Nom) : le nom de l'interface, jusqu'à 48 caractères. Si vous modifiez le nom d'une interface existante, il est automatiquement mis à jour dans toutes les politiques et tous les objets qui l'incluent. Vous ne pouvez pas utiliser de lettres majuscules dans le nom.
- **Status** (État) : cliquez sur le curseur pour le mettre en position Enabled (Activé) .
- **Description** : (facultatif.) La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).
- **Tunnel ID** (ID du tunnel) : un nombre de 0 à 10 413. Ce numéro est ajouté au mot Tunnel pour former le nom matériel de l'interface. Vous devez choisir un numéro que vous n'avez pas déjà utilisé pour une autre VTI. Par exemple, saisissez 1 pour créer l'interface Tunnel1.
- **Tunnel Source** (Source du tunnel) : sélectionnez l'interface associée à cette VTI. La source du tunnel est l'interface par laquelle le VPN site à site défini sur l'interface de tunnel virtuel se connectera au point de terminaison distant. Sélectionnez une interface qui peut atteindre le point de terminaison distant, par exemple l'interface outside. L'interface source peut être une interface physique, une sous-interface ou un EtherChannel, et elle doit avoir un nom. L'interface ne peut pas être membre d'une interface virtuelle de pont (BVI).
- **IP Address and Subnet Mask (Adresse IP et masque de sous-réseau)** : l'adresse IPv4 et le masque de sous-réseau associé. Par exemple, 192.168.1.1/24 ou /255.255.255.0. Cette adresse n'a pas besoin d'être sur le même sous-réseau que l'adresse de l'interface source du tunnel. Toutefois, si vous configurez un VPN d'accès à distance (RA) sur l'interface source, l'adresse IP de la VTI ne peut pas se trouver dans le pool d'adresses configuré pour le VPN RA.

Étape 4 Cliquez sur **OK**.

Autoriser le trafic via le VPN de site à site

Vous pouvez utiliser l'une des techniques suivantes pour activer la circulation du trafic dans le tunnel VPN de site à site.

- Configurez la commande **sysopt connection permit-vpn**, qui exempte le trafic qui correspond à la connexion VPN de la politique de contrôle d'accès. La valeur par défaut pour cette commande est **no sysopt connection permit-vpn**, ce qui signifie que le trafic VPN doit également être autorisé par la politique de contrôle d'accès.

  Il s'agit de la méthode la plus sécurisée pour autoriser le trafic dans le VPN, car les utilisateurs externes ne peuvent pas falsifier des adresses IP dans le réseau protégé distant. L'inconvénient est que le trafic VPN ne sera pas inspecté, ce qui signifie que la protection contre les intrusions et les fichiers, le filtrage des URL ou d'autres fonctions avancées ne seront pas appliqués au trafic. Cela signifie également qu'aucun événement de connexion ne sera généré pour le trafic, et donc les tableaux de bord statistiques ne refléteront pas les connexions VPN.

  La méthode préférée pour configurer cette commande est de créer un profil de connexion VPN d'accès à distance dans lequel vous sélectionnez l'option **Bypass Access Control** (contournement du contrôle d'accès) pour le trafic déchiffré. Si vous ne souhaitez pas configurer le VPN d'accès à distance ou si vous ne pouvez pas configurer le VPN d'accès à distance, vous pouvez utiliser FlexConfig pour configurer la commande.

Remarque Cette méthode ne s'applique pas aux connexions VPN basées sur le routage configurées sur une Virtual Tunnel Interface (interface de tunnel virtuel) (VTI). Vous devez toujours configurer les règles de contrôle d'accès pour les VPN basés sur le routage.

- Créez des règles de contrôle d'accès pour autoriser les connexions à partir du réseau distant. Cette méthode garantit que le trafic VPN est inspecté et que des services avancés peuvent être appliqués aux connexions. L'inconvénient est que des utilisateurs externes ont alors la possibilité de falsifier les adresses IP et d'accéder ainsi à votre réseau interne.

Configuration de la politique IKE globale

L'Internet Key Exchange (IKE ou l'échange de clé Internet) est un protocole de gestion de clés utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec.

La négociation IKE comprend deux phases. La phase 1 négocie une association de sécurité entre deux homologues IKE, ce qui permet aux homologues de communiquer de manière sécurisée pendant la phase 2. Pendant la négociation de la phase 2, IKE établit les associations de sécurité pour d'autres applications, telles qu'IPsec. Les deux phases utilisent des propositions lorsqu'elles négocient une connexion. Une proposition IKE est un ensemble d'algorithmes que deux homologues utilisent pour sécuriser la négociation entre eux. La négociation IKE commence lorsque chaque homologue s'accorde sur une politique IKE commune (partagée). Cette politique énonce les paramètres de sécurité utilisés pour protéger les négociations IKE ultérieures.

Les objets de politique IKE définissent les propositions IKE pour ces négociations. Les objets que vous activez sont ceux utilisés lorsque les homologues négocient une connexion VPN : vous ne pouvez pas spécifier différentes politiques IKE par connexion. La priorité relative de chaque objet détermine quelles politiques sont essayées en premier, le nombre le plus bas correspondant à la priorité la plus élevée. La connexion n'est pas établie si la négociation ne parvient pas à trouver une politique que les deux homologues puissent prendre en charge.

Pour définir la politique IKE globale, vous sélectionnez les objets à activer pour chaque version IKE. Si les objets prédéfinis ne satisfont pas vos exigences, créez de nouvelles politiques pour appliquer votre politique de sécurité.

La procédure suivante explique comment configurer la politique globale à l'aide de la page Objets. Vous pouvez également activer, désactiver et créer des politiques lors de la modification d'une connexion VPN en cliquant sur **Edit** (Modifier) dans les paramètres de politique IKE.

Remarque Vous pouvez activer jusqu'à 20 politiques IKE.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **IKE Policies** (Politiques IKE) dans la table des matières.

Les politiques pour IKEv1 et IKEv2 sont affichées dans des listes distinctes.

Étape 2 Activez les politiques IKE que vous souhaitez autoriser pour chaque version IKE.

a) Sélectionnez **IKEv1** ou **IKEv2** au-dessus de la table d'objets pour afficher les politiques de cette version.

b) Cliquez sur la bascule **State** (État) pour activer les objets appropriés et désactiver ceux qui ne répondent pas à vos besoins.

Si certaines de vos exigences de sécurité ne sont pas reflétées dans les objets existants, définissez-en de nouveaux pour les mettre en œuvre. Pour plus de détails, consultez les rubriques suivantes :

- Configuration des politiques IKEv1, à la page 675
- Configuration des politiques IKEv2, à la page 677

c) Vérifiez que les priorités relatives correspondent à vos besoins.

Si vous devez modifier la priorité d'une politique, modifiez-la. S'il s'agit d'une politique système prédéfinie, vous devez créer votre propre version de la politique pour modifier la priorité.

La priorité est relative et non absolue. Par exemple, la priorité 80 est supérieure à 160. Si 80 est l'objet ayant la priorité la plus élevée que vous activez, cela devient votre politique de premier choix. Si vous activez ensuite une politique de priorité 25, elle devient votre politique de premier choix.

d) Si vous utilisez les deux versions IKE, répétez le processus pour l'autre version.

Configuration des politiques IKEv1

Les objets de politique Internet Key Exchange (IKE), version 1 contiennent les paramètres requis pour les politiques IKEv1 lors de la définition des connexions VPN. IKE est un protocole de gestion de clés qui facilite la gestion des communications basées sur IPsec. Il est utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec (SA).

Il existe plusieurs politiques IKEv1 prédéfinies. Si certaines répondent à vos besoins, activez-les simplement en cliquant sur le bouton à bascule **State** (État). Vous pouvez également créer des politiques pour mettre en œuvre d'autres combinaisons de paramètres de sécurité. Vous ne pouvez pas modifier ou supprimer des objets définis par le système.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de politique IKEv1 lors de la modification des paramètres IKEv1 dans une connexion VPN en cliquant sur le lien **Create New IKE Policy** (Créer une nouvelle politique IKE) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **IKE Policies** (Politiques IKE) dans la table des matières.

Étape 2 Sélectionnez **IKEv1** au-dessus de la table d'objets pour afficher les politiques IKEv1.

Étape 3 Si l'une des politiques définies par le système répond à vos besoins, cliquez sur la bascule **State** (État) pour les activer.

Utilisez également la bascule **State** (État) pour désactiver les politiques indésirables. La priorité relative de chaque objet détermine lesquelles de ces politiques sont essayées en premier, le nombre le plus bas étant une priorité la plus élevée.

Étape 4 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 5 Configurez les propriétés IKEv1.

- **Priority**(Priorité) : Priorité : priorité relative de la politique IKE, de 1 à 65 535. La priorité détermine l'ordre de la politique IKE par rapport aux deux homologues négociateurs lors de la tentative de trouver une association de sécurité (SA) commune. Si l'homologue IPsec distant ne prend pas en charge les paramètres sélectionnés dans votre politique de priorité la plus élevée, il essaie d'utiliser les paramètres définis dans la prochaine priorité la plus basse. Plus le numéro de priorité est faible, plus la priorité est élevée.
- **Name** (Nom) : Le nom de l'objet, jusqu'à 128 caractères.
- **State**(État) : État : indique si la politique IKE est activée ou désactivée. Cliquez sur le bouton à bascule pour modifier l'état. Seules les politiques activées sont utilisées pendant les négociations IKE.
- **Authentification** : la méthode d'authentification à utiliser entre les deux homologues. Pour obtenir plus de renseignements, consultez Choix de la méthode d'authentification à utiliser, à la page 663.
  - **Clé prépartagée** : utilisez la clé prépartagée définie sur chaque périphérique. Ces clés permettent de partager une clé secrète entre deux homologues et d'être utilisée par IKE pendant la phase d'authentification. Si l'homologue n'est pas configuré avec la même clé prépartagée, le SA IKE ne peut pas être établi.
  - **Certificat)** : utilisez les certificats d'identité d'appareil pour les homologues pour s'identifier. Vous devez obtenir ces certificats en inscrivant chaque homologue dans une autorité de certification. Vous devez également télécharger la racine de l'autorité de certification et les certificats intermédiaires de l'autorité de certification de confiance utilisés pour signer les certificats d'identité chez chaque homologue. Les homologues peuvent être inscrits dans la même autorité de certification ou dans une autre autorité de certification. Vous ne pouvez pas utiliser de certificats autosignés pour l'un ou l'autre des homologues.
- **Chiffrement** : l'algorithme de chiffrement utilisé pour établir l'association de sécurité (SA) de phase 1 en vue de protéger les négociations de la phase 2. Pour obtenir une explication des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 661.
- **Groupe Diffie-Hellman** : le groupe Diffie-Hellman à utiliser pour obtenir un secret partagé entre les deux homologues IPsec sans le transmettre l'un à l'autre. Un module plus élevé offre une sécurité supérieure, mais nécessite plus de temps de traitement. Les deux homologues doivent avoir un groupe de module correspondant. Pour obtenir une explication des options, consultez Choix du groupe de module Diffie-Hellman à utiliser, à la page 662.
- **Hachage** : l'algorithme de hachage pour créer un condensé de message, qui est utilisé pour assurer l'intégrité du message. Pour obtenir une explication des options, consultez Décider des algorithmes de hachage à utiliser, à la page 662.
- **Lifetime** (Durée de vie) :Durée de vie : la durée de vie de l'association de sécurité (SA), en secondes, de 120 à 2 147 483 647 ou vide. Lorsque la durée de vie est dépassée, l'association de sécurité expire et doit être renégociée entre les deux homologues. En règle générale, plus la durée de vie est courte (jusqu'à

un certain point), plus vos négociations IKE seront sécurisées. Cependant, avec des durées de vie plus longues, les futures associations de sécurité IPsec peuvent être configurées plus rapidement qu'avec des durées de vie plus courtes. La valeur par défaut est 86 400. Pour spécifier une durée de vie illimitée, ne saisissez aucune valeur (laissez le champ vide).

Étape 6 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des politiques IKEv2

Les objets de politique Internet Key Exchange (IKE) version 2 contiennent les paramètres requis pour les politiques IKEv2 lors de la définition des connexions VPN. IKE est un protocole de gestion de clés qui facilite la gestion des communications basées sur IPsec. Il est utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec (SA).

Il existe plusieurs politiques IKEv2 prédéfinies. Si certaines répondent à vos besoins, activez-les simplement en cliquant sur le bouton à bascule **State** (État). Vous pouvez également créer des politiques pour mettre en œuvre d'autres combinaisons de paramètres de sécurité. Vous ne pouvez pas modifier ou supprimer des objets définis par le système.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer une politique IKEv2 lors de la modification des paramètres IKE dans une connexion VPN de site à site en cliquant sur le lien **Create New IKEv2 Policy** (Créer une nouvelle politique IKEv2) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Politiques IKE** dans la table des matières.

Étape 2 Sélectionnez **IKEv2** au-dessus de la table d'objets pour afficher les politiques IKEv2.

Étape 3 Si l'une des politiques définies par le système répond à vos besoins, cliquez sur la bascule **State** (État) pour les activer.

Utilisez également la bascule **State** (État) pour désactiver les politiques indésirables. La priorité relative de chaque objet détermine lesquelles de ces politiques sont essayées en premier, le nombre le plus bas étant une priorité la plus élevée.

Étape 4 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 5 Configurez les propriétés IKEv2.

- **Priority**(Priorité) : Priorité : priorité relative de la politique IKE, de 1 à 65 535. La priorité détermine l'ordre de la politique IKE par rapport aux deux homologues négociateurs lors de la tentative de trouver une association de sécurité (SA) commune. Si l'homologue IPsec distant ne prend pas en charge les paramètres sélectionnés dans votre politique de priorité la plus élevée, il essaie d'utiliser les paramètres

définis dans la prochaine priorité la plus basse. Plus le numéro de priorité est faible, plus la priorité est élevée.

- **Name** (Nom) : Le nom de l'objet, jusqu'à 128 caractères.
- **State**(État) : État : indique si la politique IKE est activée ou désactivée. Cliquez sur le bouton à bascule pour modifier l'état. Seules les politiques activées sont utilisées pendant les négociations IKE.
- **Chiffrement** : l'algorithme de chiffrement utilisé pour établir l'association de sécurité (SA) de phase 1 en vue de protéger les négociations de la phase 2. Sélectionnez tous les algorithmes que vous souhaitez autoriser, bien que vous ne puissiez pas inclure les options de mode mixte (AES-GCM) et de mode normal dans la même politique. (Le mode normal exige que vous sélectionniez un hachage d'intégrité, tandis que le mode mixte interdit une sélection de hachage d'intégrité distincte.) Le système négocie avec l'homologue, en commençant par l'algorithme le plus fort vers l'algorithme le plus faible, jusqu'à ce qu'une correspondance soit trouvée. Pour obtenir une explication des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 661.
- **Groupe Diffie-Hellman** : le groupe Diffie-Hellman à utiliser pour obtenir un secret partagé entre les deux homologues IPsec sans le transmettre l'un à l'autre. Un module plus élevé offre une sécurité supérieure, mais nécessite plus de temps de traitement. Les deux homologues doivent avoir un groupe de module correspondant. Sélectionnez tous les algorithmes que vous souhaitez autoriser. Le système négocie avec l'homologue, en commençant par le groupe le plus fort vers le plus faible jusqu'à ce qu'une correspondance soit trouvée. Pour obtenir une explication des options, consultez Choix du groupe de module Diffie-Hellman à utiliser, à la page 662.
- **Integrity Hash** (hachage d'intégrité) : la partie intégrité de l'algorithme de hachage pour la création d'un condensé de message, qui est utilisée pour assurer l'intégrité du message. Sélectionnez tous les algorithmes que vous souhaitez autoriser. Le système négocie avec l'homologue, en commençant par l'algorithme le plus fort vers l'algorithme le plus faible, jusqu'à ce qu'une correspondance soit trouvée. Le hachage d'intégrité n'est pas utilisé avec les options de chiffrement AES-GCM. Pour obtenir une explication des options, consultez Décider des algorithmes de hachage à utiliser, à la page 662.
- **Pseudo-Random Function (PRF) Hash** (hachage de la fonction pseudo-aléatoire (PRF)) : la partie fonction pseudo-aléatoire (PRF) de l'algorithme de hachage, qui est utilisée comme algorithme pour dériver le matériel de clé et les opérations de hachage requises pour le chiffrement du tunnel IKEv2. Dans IKEv1, les algorithmes d'intégrité et de PRF ne sont pas séparés, mais dans IKEv2, vous pouvez spécifier des algorithmes différents pour ces éléments. Sélectionnez tous les algorithmes que vous souhaitez autoriser. Le système négocie avec l'homologue, en commençant par l'algorithme le plus fort vers l'algorithme le plus faible, jusqu'à ce qu'une correspondance soit trouvée. Pour obtenir une explication des options, consultez Décider des algorithmes de hachage à utiliser, à la page 662.
- **Lifetime** (Durée de vie) :Durée de vie : la durée de vie de l'association de sécurité (SA), en secondes, de 120 à 2 147 483 647 ou vide. Lorsque la durée de vie est dépassée, l'association de sécurité expire et doit être renégociée entre les deux homologues. En règle générale, plus la durée de vie est courte (jusqu'à un certain point), plus vos négociations IKE seront sécurisées. Cependant, avec des durées de vie plus longues, les futures associations de sécurité IPsec peuvent être configurées plus rapidement qu'avec des durées de vie plus courtes. La valeur par défaut est 86 400. Pour spécifier une durée de vie illimitée, ne saisissez aucune valeur (laissez le champ vide).

Étape 6 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des propositions IPsec

IPsec est l'une des méthodes les plus sécurisées de configuration d'un VPN. La fonctionnalité IPsec de Cisco IOS fournit le chiffrement de données réseau au niveau des paquets IP et offre une solution de sécurité robuste basée sur des normes. Grâce à IPsec, les données sont transmises sur un réseau public par l'intermédiaire de tunnels. Un tunnel est un chemin de communication logique et sécurisé entre deux homologues. Le trafic qui entre dans un tunnel IPsec est sécurisé par une combinaison d'algorithmes et de protocoles de sécurité appelée ensemble de transformations. Pendant la négociation d'association de sécurité (SA) d'IPsec, les homologues recherchent un ensemble de transformations identique sur les deux homologues.

Il existe des objets de proposition IPsec distincts selon la version IKE, IKEv1 ou IKEv2 :

- Lorsque vous créez une proposition IKEv1, vous sélectionnez le mode de fonctionnement d'IPsec et définissez les types de chiffrement et d'authentification requis. Vous pouvez sélectionner une seule option pour les algorithmes. Si vous souhaitez prendre en charge plusieurs combinaisons dans un VPN, créez et sélectionnez plusieurs objets Proposition IKEv1 IPsec.
- Lorsque vous créez une proposition IKEv2 IPsec, vous pouvez sélectionner tous les algorithmes de chiffrement et de hachage autorisés dans un VPN. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue jusqu'à ce qu'une correspondance soit trouvée. Cela vous permet d'envoyer potentiellement une seule proposition pour transmettre toutes les combinaisons autorisées au lieu d'avoir besoin d'envoyer chaque combinaison autorisée individuellement, comme avec IKEv1.

Le protocole ESP (Encapsulating Security Protocol) est utilisé pour les propositions d'IPsec IKEv1 et IKEv2. Il fournit des services d'authentification, de chiffrement et d'antirelecture. ESP est un protocole IP de type 50.



Remarque Nous vous recommandons d'utiliser à la fois le chiffrement et l'authentification sur les tunnels IPsec.

Les rubriques suivantes expliquent comment configurer les propositions IPsec pour chaque version d'IKE :

Configuration des propositions IPsec pour IKEv1

Utilisez les objets IKEv1 IPsec Proposal (proposition IPsec IKEv1) pour configurer la proposition IPsec utilisée lors des négociations de la phase 2 d'IKE. La proposition IPsec définit la combinaison de protocoles et d'algorithmes de sécurité qui sécurisent le trafic dans un tunnel IPsec.

Il existe plusieurs propositions IKEv1 IPsec prédéfinies. Vous pouvez également créer de nouvelles propositions pour mettre en œuvre d'autres combinaisons de paramètres de sécurité. Vous ne pouvez pas modifier ou supprimer des objets définis par le système.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets IKEv1 IPsec Proposals (propositions IKEv1 IPsec) tout en modifiant les paramètres IKEv1 IPsec dans une connexion VPN, en cliquant sur le lien **Create New IPsec Proposal** (Créer une nouvelle proposition IPsec) affiché dans la liste des objets.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **IPsec Proposals** (propositions IPsec) dans la table des matières.

Étape 2 Sélectionnez **IKEv1** au-dessus de la table des objets pour afficher les propositions IKEv1 IPsec.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Configurez les propriétés de la proposition IPsec IKEv1.

- **Name (Nom)**—Le nom de l'objet, jusqu'à 128 caractères.
- **Mode** : le mode dans lequel fonctionne le tunnel IPSec.
  - Le mode **Tunnel** encapsule l'ensemble du paquet IP. L'en-tête IPSec est ajouté entre l'en-tête IP d'origine et le nouvel en-tête IP. Il s'agit du paramètre par défaut. Utilisez le mode tunnel lorsque le pare-feu protège le trafic vers et en provenance des hôtes situés derrière le pare-feu. Le mode tunnel est la façon dont le protocole IPSec standard est mis en œuvre entre deux pare-feu (ou autres passerelles de sécurité) qui sont connectés sur un réseau non fiable, comme Internet.
  - Le mode **Transport** encapsule uniquement les protocoles des couches supérieures d'un paquet IP. L'en-tête IPSec est inséré entre l'en-tête IP et l'en-tête de protocole de la couche supérieure (comme TCP). Le mode de transport nécessite que les hôtes source et de destination prennent en charge IPSec et ne peut être utilisé que lorsque l'homologue de destination du tunnel est la destination finale du paquet IP. Le mode de transport est généralement utilisé uniquement pour la protection d'un protocole de tunnellisation de couche 2 ou de couche 3 comme GRE, L2TP et DLSW.
- **ESP Encryption** (Chiffrement ESP) : algorithme de chiffrement Encapsulating Security Protocol (ESP) pour cette proposition. Pour obtenir une explication des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 661.
- **ESP Hash (Hachage ESP)** : algorithme de hachage ou d'intégrité à utiliser pour l'authentification. Pour obtenir une explication des options, consultez Décider des algorithmes de hachage à utiliser, à la page 662.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des propositions IPsec pour IKEv2

Les objets Proposition IPsec IKEv2 configurent la proposition IPsec utilisée lors des négociations de la phase 2 d'IKE. La proposition IPsec définit la combinaison de protocoles et d'algorithmes de sécurité qui sécurisent le trafic dans un tunnel IPsec.

Il existe plusieurs propositions IKEv2 IPsec prédéfinies. Vous pouvez également créer de nouvelles propositions pour mettre en œuvre d'autres combinaisons de paramètres de sécurité. Vous ne pouvez pas modifier ou supprimer des objets définis par le système.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de propositions IKEv2 IPsec tout en modifiant les paramètres IKEv2 IPsec dans une connexion VPN en cliquant sur le lien **Créer une nouvelle proposition IPsec** dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (objets), puis **IPsec Proposals** (propositions IPsec) dans la table des matières.

Étape 2 Sélectionnez **IKEv2** au-dessus de la table des objets pour afficher les propositions IPsec IKEv2.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Configurez les propriétés de la proposition IPsec IKEv2.

- **Nom**—Le nom de l'objet, jusqu'à 128 caractères.
- **Chiffrement** : l'algorithme de chiffrement Encapsulating Security Protocol (ESP) pour cette proposition. Sélectionnez tous les algorithmes que vous souhaitez autoriser. Le système négocie avec l'homologue, en commençant par l'algorithme le plus fort vers l'algorithme le plus faible, jusqu'à ce qu'une correspondance soit trouvée. Pour obtenir une explication des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 661.
- **Hachage d'intégrité** : l'algorithme de hachage ou d'intégrité à utiliser pour l'authentification. Sélectionnez tous les algorithmes que vous souhaitez autoriser. Le système négocie avec l'homologue, en commençant par l'algorithme le plus fort vers l'algorithme le plus faible, jusqu'à ce qu'une correspondance soit trouvée. Pour obtenir une explication des options, consultez Décider des algorithmes de hachage à utiliser, à la page 662.

  Remarque
  Cependant, vous devez choisir l'algorithme d'intégrité nulle si vous sélectionnez l'une des options AES-GCM/GMAC comme algorithme de chiffrement. Même si vous choisissez une option non nulle, le hachage d'intégrité est ignoré pour ces normes de chiffrement.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Vérification des connexions VPN de site à site

Après avoir configuré une connexion VPN de site à site et déployé la configuration sur le périphérique, vérifiez que le système établit l'association de sécurité avec le périphérique distant.

Si la connexion ne peut pas être établie, utilisez la commande **ping interface** *interface_name remote_ip_address* de l'interface de ligne de commande du périphérique pour vous assurer qu'il existe un chemin dans l'interface VPN vers le périphérique distant. S'il n'y a aucune connexion par l'intermédiaire de l'interface configurée, vous pouvez ignorer le mot-clé **interface** *interface_name* et déterminer si la connectivité se fait par l'intermédiaire d'une interface différente. Vous avez peut-être sélectionné la mauvaise interface pour la connexion : vous devez sélectionner l'interface qui fait face au périphérique distant, et non l'interface qui fait face au réseau protégé.

S'il existe un chemin réseau, vérifiez les versions et les clés IKE configurées et prises en charge par les deux points terminaux, et ajustez la connexion VPN au besoin. Assurez-vous qu'aucune règle de contrôle d'accès ou de NAT ne bloque la connexion.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande du périphérique comme expliqué dans Connexion avec l'interface de ligne de commande (CLI), à la page 18.

Étape 2 Utilisez la commande **show ipsec sa** pour vérifier que l'association de sécurité IPsec est établie.

Vous devriez voir que la connexion VPN est établie entre votre périphérique (l'**adresse locale**) et l'homologue distant (**current_peer**). Le nombre de paquets (pkts) devrait augmenter à mesure que vous envoyez du trafic par la connexion. La liste d'accès doit afficher les réseaux locaux et distants pour la connexion.

Par exemple, la sortie suivante montre une connexion IKEv2.

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
      #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/500, remote crypto endpt.: 192.168.4.6/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CD22739C
      current inbound spi : 52D2F1E4

    inbound esp sas:
      spi: 0x52D2F1E4 (1389556196)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4285434/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xCD22739C (3441587100)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
```

```
        in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
        slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
        sa timing: remaining key lifetime (kB/sec): (4055034/28730)
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

La sortie suivante montre une connexion IKEv1.

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
      #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/0, remote crypto endpt.: 192.168.4.6/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 077D72C9
      current inbound spi : AC146DEC

    inbound esp sas:
      spi: 0xAC146DEC (2887020012)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
         slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (3914999/28567)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x000007FF
    outbound esp sas:
      spi: 0x077D72C9 (125661897)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
         slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (3914999/28567)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Étape 3 Utilisez la commande **show isakmp sa** pour vérifier les associations de sécurité IKE.

Vous pouvez utiliser la commande sans le mot-clé **sa** (ou utiliser le mot-clé **stats** à la place) pour afficher les statistiques IKE.

Par exemple, la sortie suivante affiche une association de sécurité IKEv2.

```
> show isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:15317, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local             Remote            Status   Role
592216161 192.168.2.15/500  192.168.4.6/500   READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x52d2f1e4/0xcd22739c
```

Le résultat suivant montre une association de sécurité IKEv1.

```
> show isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.4.6
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
```

Supervision du VPN de site à site

Pour superviser et dépanner les connexions VPN de site à site, ouvrez la console d'interface en ligne de commande ou connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes.

- **show ipsec sa** affiche les sessions VPN (associations de sécurité). Vous pouvez réinitialiser ces statistiques à l'aide de la commande **clear ipsec sa counters**.
- **show ipsec** *keyword* affiche les données et les statistiques opérationnelles IPsec. Saisissez **show ipsec ?** pour afficher les mots-clés disponibles.
- **show isakmp** affiche les données et les statistiques opérationnelles d'ISAKMP.

Exemples de VPN de site à site

Voici des exemples de configuration d'un VPN de site à site.

Exemption du trafic VPN de site à site de la NAT

Lorsque vous avez une connexion VPN de site à site définie sur une interface, et que vous avez également des règles NAT pour cette interface, vous pouvez éventuellement exempter le trafic sur le VPN des règles NAT. Vous souhaiterez peut-être le faire si l'extrémité distante de la connexion VPN peut gérer vos adresses internes.

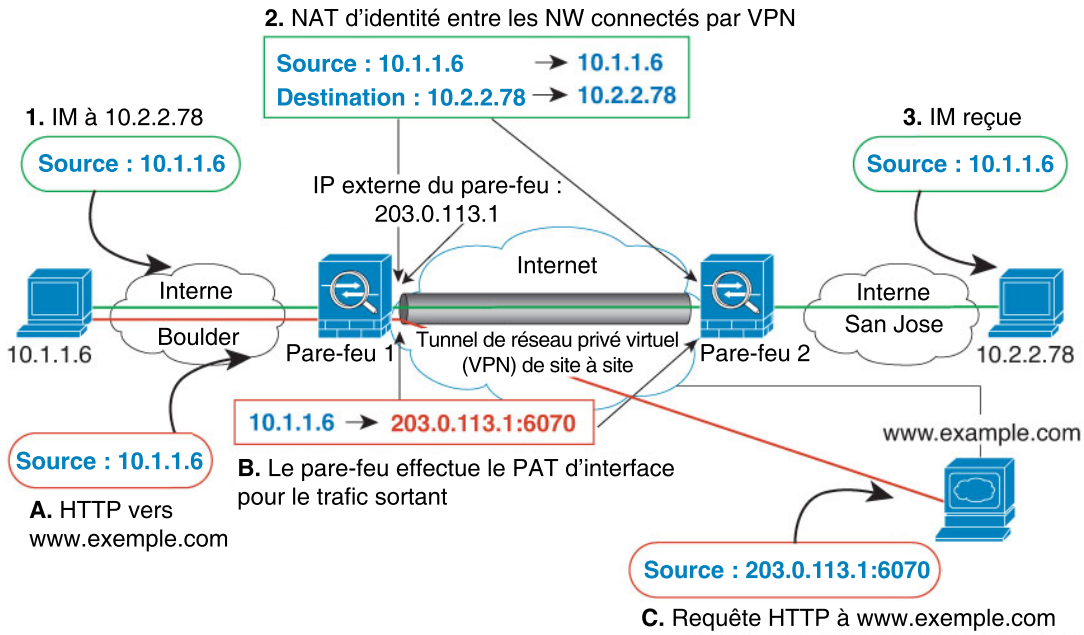
Lorsque vous créez la connexion VPN, vous pouvez sélectionner l'option d'**exemption de NAT** pour créer les règles automatiquement. Cependant, cela ne fonctionne que si votre réseau local protégé est connecté par l'intermédiaire d'une interface à routage unique (et non un membre d'un groupe de ponts). Si, au contraire, les réseaux locaux de la connexion se trouvent derrière au moins deux interfaces de routage ou un ou plusieurs membres de groupes de ponts, vous devez configurer manuellement les règles d'exemption NAT.

Pour exempter le trafic VPN des règles NAT, vous créez une règle NAT manuelle d'identité pour le trafic local lorsque la destination est le réseau distant. Ensuite, appliquez la NAT au trafic lorsque la destination est autre chose (par exemple, Internet). Si vous avez plusieurs interfaces pour le réseau local, créez des règles pour chaque interface. Tenez également compte des suggestions suivantes :

- S'il y a plusieurs réseaux locaux dans la connexion, créez un groupe d'objets réseau pour contenir les objets qui définissent les réseaux.
- Si vous incluez à la fois des réseaux IPv4 et IPv6 dans le VPN, créez des règles NAT d'identité distinctes pour chacun.

Considérez l'exemple suivant, qui montre un tunnel de site à site connectant les bureaux de Bouder et de San José. Pour le trafic que vous souhaitez diriger vers Internet (par exemple, de la section 10.1.1.6 à Boulder vers www.exemple.com), vous avez besoin d'une adresse IP publique fournie par la NAT pour accéder à Internet. L'exemple ci-dessous utilise les règles PAT d'interface. Cependant, pour le trafic que vous souhaitez acheminer par le tunnel VPN (par exemple, de la version 10.1.1.6 à Boulder au 10.2.2.78 à San Jose), vous ne souhaitez pas effectuer la NAT; vous devez exclure ce trafic en créant une règle NAT d'identité. La NAT d'identité traduit simplement une adresse en la même adresse.

Illustration 25 : PAT d'interface et NAT d'identité pour le VPN de site à site



L'exemple suivant explique la configuration de Firewall1 (Boulder). Cet exemple suppose que l'interface interne est un groupe de ponts. Vous devez donc écrire les règles pour chaque interface membre. Le processus est le même si vous avez une ou plusieurs interfaces internes routées.

Remarque Cet exemple suppose qu'il s'agit d'un protocole IPv4 uniquement. Si le VPN comprend également des réseaux IPv6, créez des règles parallèles pour IPv6. Notez que vous ne pouvez pas implémenter l'interface PAT pour IPv6, vous devez donc créer un objet hôte avec une adresse IPv6 unique à utiliser pour la PAT.

Procédure

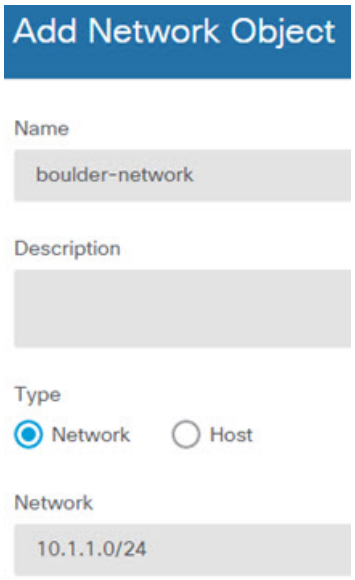
Étape 1 Créez les objets pour définir les différents réseaux.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.

c) Repérez le réseau interne Boulder.

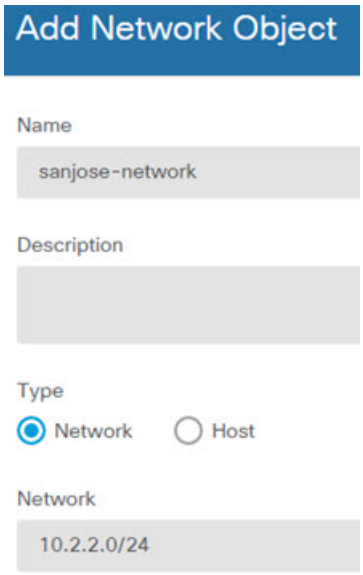
Nommez l'objet réseau (par exemple, boulder-network), sélectionnez **Network** (Réseau) et saisissez l'adresse réseau, 10.1.1.0/24.



d) Cliquez sur **OK**.

e) Cliquez sur + et définissez le réseau interne de San Jose.

Nommez l'objet réseau (par exemple, sanjose-network), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau 10.2.2.0/24.



f) Cliquez sur **OK**.

Étape 2 Configurer la NAT d'identité manuelle pour le réseau Boulder lorsqu'il passe par le VPN vers San Jose sur le Firewall1 (Boulder).

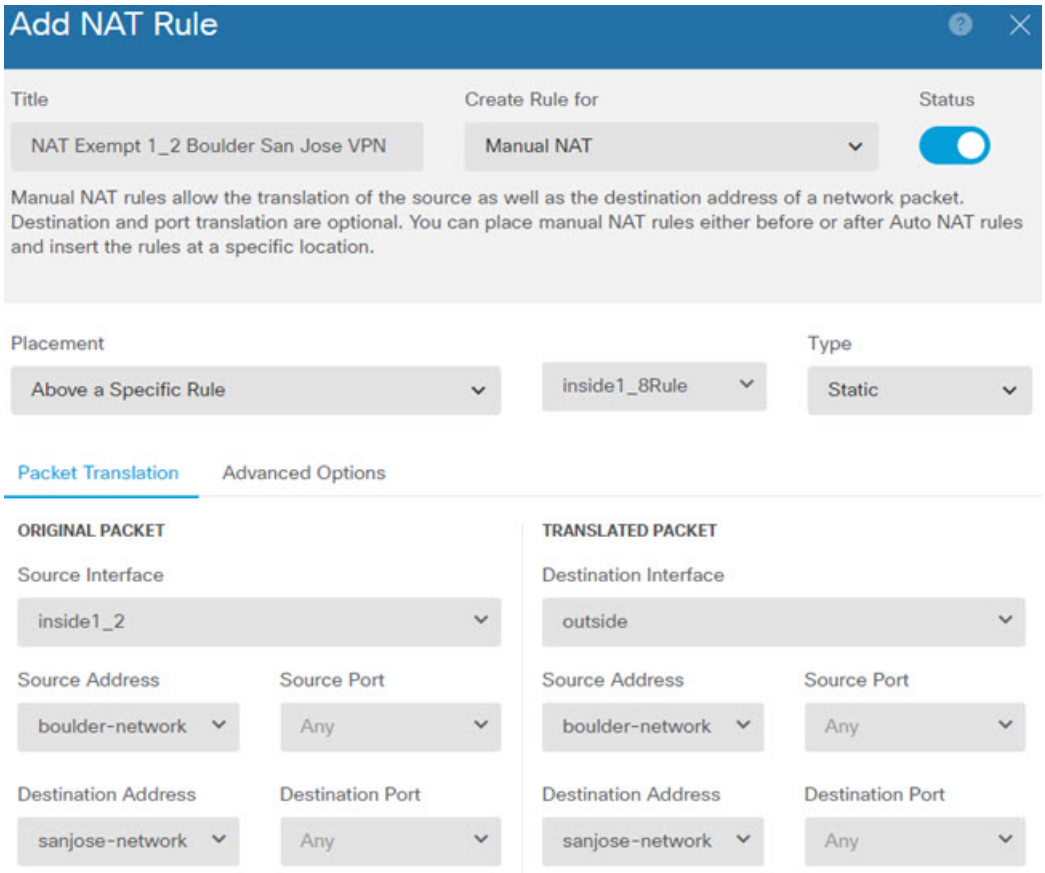
a) Sélectionnez **Policies (Politiques)** > **NAT**.

b) Cliquez sur le bouton +.

c) Configurez les propriétés suivantes :

- **Titre** = NAT Exempt 1_2 Boulder San Jose VPN (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Placement** (Emplacement) = **Above a Specific Rule** (Au-dessus d'une règle spécifique), et sélectionnez la première règle dans la section NAT manuelle avant NAT automatique. Vous voulez vous assurer que cette règle précède toutes les règles PAT d'interface générales pour l'interface de destination. Sinon, la règle pourrait ne pas être appliquée au bon trafic.
- **Type** = Statique.
- **Interface source** = inside1_2.
- **Interface de destination** = externe.
- **Adresse source d'origine** = objet boulder-network.
- **Adresse source traduite** = objet boulder-network.
- **Adresse de destination d'origine** = objet sanjose-network.
- **Adresse de destination traduite** = objet sanjose-network.

Remarque
Comme vous ne souhaitez pas traduire l'adresse de destination, vous devez configurer la NAT d'identité en utilisant la même adresse pour les adresses de destination originale et traduite. Laissez tous les champs de port vides. Cette règle configure la NAT d'identité pour la source et la destination.



d) Dans l'onglet **Advanced** (Avancé), sélectionnez **Do not proxy ARP on Destination interface** (Désactiver le mandataire ARP sur l'interface de destination).
e) Cliquez sur **OK**.
f) Répétez le processus pour créer des règles équivalentes pour chacune des autres interfaces internes.

Étape 3 Configurez manuellement l'interface dynamique PAT lors de la connexion à Internet pour le réseau interne Boulder sur Firewall1 (Boulder).

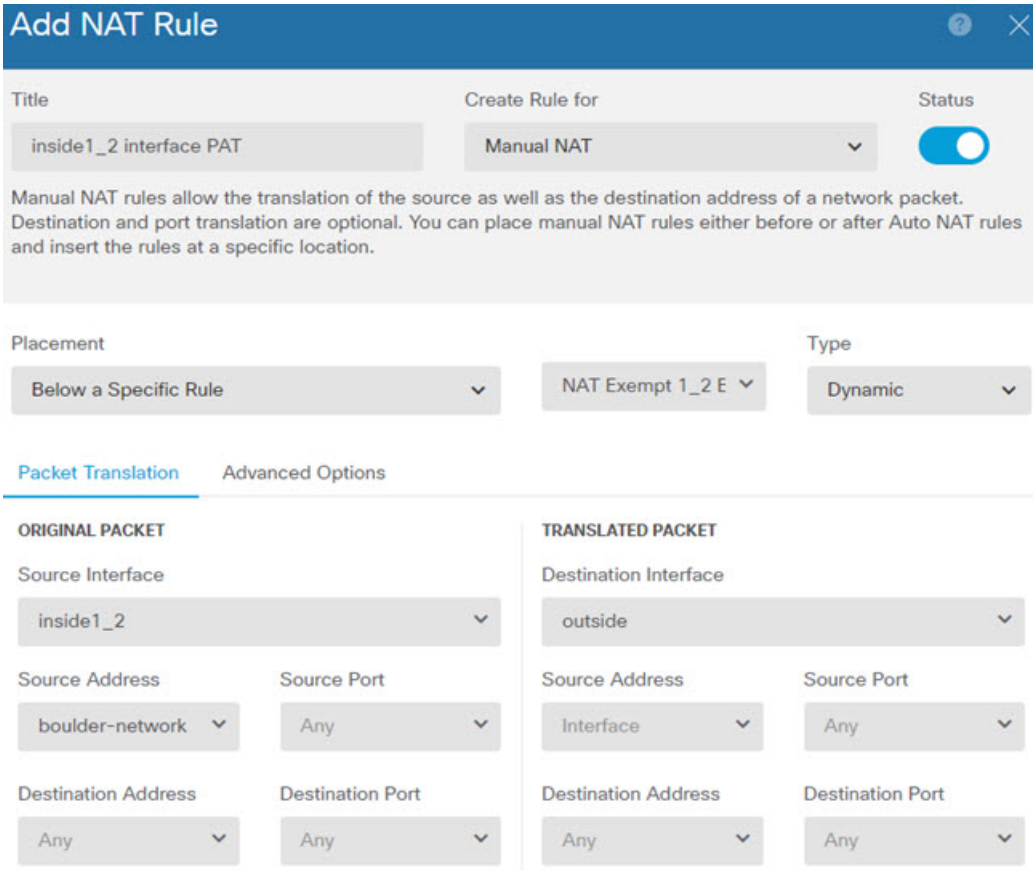
Remarque
Remarque : Il existe peut-être déjà des règles PAT d'interface dynamique pour les interfaces internes, couvrant tout trafic IPv4, car celles-ci sont créées par défaut lors de la configuration initiale. Cependant, la configuration est affichée ici par souci d'exhaustivité. Avant de suivre ces étapes, vérifiez si une règle existe déjà qui couvre l'interface interne et le réseau, et ignorez cette étape si c'est le cas.

a) Cliquez sur le bouton +.
b) Configurez les propriétés suivantes :

- **Title** (Titre) = interface PAT inside1_2 (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Placement** (Emplacement) = **Below a Specific Rule** (Ci-dessous une règle spécifique), et sélectionnez la première règle dans la section NAT manuelle avant NAT automatique. Étant donné que cette règle s'applique à toute adresse de destination, la règle qui utilise sanjose-network comme destination doit précéder cette règle, sinon la règle sanjose-network ne sera jamais mise en correspondance. La

procédure par défaut est de placer les nouvelles règles NAT manuelles à la fin de la section « NAT Rules Before Auto NAT ».

- **Type** = Dynamique.
- **Interface source** = inside1_2.
- **Interface de destination** = externe.
- **Adresse source d'origine** = objet boulder-network.
- **Adresse source traduite** = **Interface**. Cette option configure l'interface PAT à l'aide de l'interface de destination.
- **Adresse de destination d'origine** = n'importe laquelle.
- **Adresse de destination traduite** = n'importe laquelle.



c) Cliquez sur **OK**.

d) Répétez le processus pour créer des règles équivalentes pour chacune des autres interfaces internes.

Étape 4 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

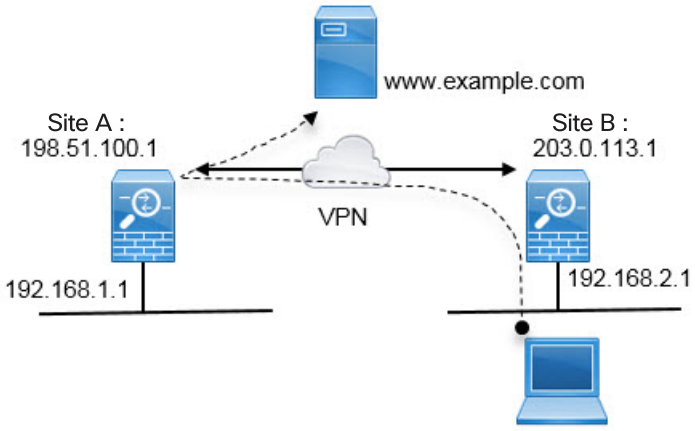
Étape 5 Si vous gérez également Firewall2 (San Jose), vous pouvez configurer des règles similaires pour ce périphérique.

- La règle de la NAT d'identité manuelle serait pour sanjose-network lorsque la destination est boulder-network. Créez de nouveaux objets d'interface pour Firewall2 , à l'intérieur et à l'extérieur des réseaux.
- La règle PAT de l'interface dynamique manuelle serait pour sanjose-network lorsque la destination est « any » (Toute).

Comment fournir un accès Internet sur l'interface externe pour les utilisateurs d'un VPN site à site externe (hairpinning)

Dans un VPN de site à site, vous pouvez souhaiter que les utilisateurs des réseaux distants accèdent à Internet par l'intermédiaire de votre périphérique. Cependant, comme les utilisateurs distants accèdent à votre périphérique sur la même interface qui fait face à Internet (l'interface externe), vous devez faire revenir le trafic Internet directement sur l'interface externe. Cette technique est appelée hairpinning.

Le graphique suivant présente un exemple. Il existe un tunnel VPN de site à site configuré entre 198.51.100.1 (sur le site principal, site A) et 203.0.113.1 (site distant, site B). Tout le trafic d'utilisateur à partir du réseau interne du site distant, 192.168.2.0/24, passe par le VPN. Ainsi, lorsqu'un utilisateur de ce réseau souhaite accéder à un serveur sur Internet, tel que www.exemple.com, la connexion passe d'abord par le VPN, puis est acheminée vers l'Internet à partir de l'interface 198.51.100.1.



La procédure suivante explique comment configurer ce service. Vous devez configurer les deux points terminaux du tunnel VPN.

Avant de commencer

Cette procédure suppose que vous utilisiez le paramètre par défaut pour autoriser le trafic VPN, ce qui applique le trafic VPN à la stratégie de contrôle d'accès. Dans la configuration en cours, cela est représenté par la commande **no sysopt connection permit-vpn**. Si vous avez plutôt activé **sysopt connection permit-vpn** par le**biais de FlexConfig ou en sélectionnant l'option de politique de contournement du contrôle d'accès pour le trafic déchiffré** dans les profils de connexion VPN d'accès à distance, les étapes de configuration des règles de contrôle d'accès ne sont pas nécessaires.

Procédure

Étape 1 (Site A, site principal.) Configurez la connexion VPN de site à site vers le site distant B.

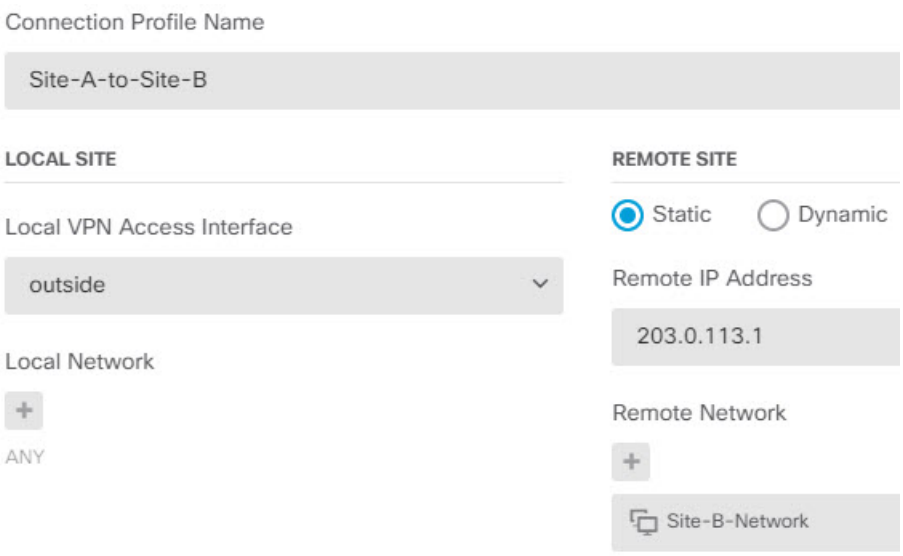
a) Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le groupe Connexion VPN de site à site.

b) Cliquez sur **+** pour ajouter une nouvelle connexion.

c) Définissez les points terminaux comme suit, puis cliquez sur **Next** (Suivant) :

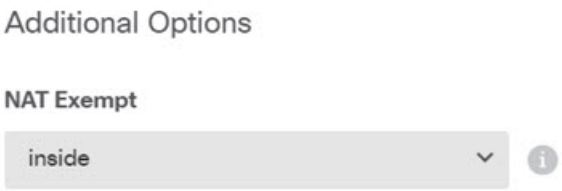
- **Connection Profile Name** (Nom du profil de connexion) : donnez à la connexion un nom significatif, par exemple Site-A-vers-Site-B.
- **Local VPN Access Interface** (Interface d'accès VPN locale) : sélectionnez l'interface externe.
- **Local Network** (Réseau local) : conservez la valeur par défaut, Any (Tout).
- **Remote IP Address** (Adresse IP distante) : saisissez l'adresse IP de l'interface externe de l'homologue distant. Dans cet exemple, 203.0.113.1.
- **Remote Network** (Réseau distant) : cliquez sur **+**, puis sélectionnez l'objet réseau qui définit le réseau protégé de l'homologue distant. Dans cet exemple, 192.168.2.0/24. Vous pouvez cliquer sur **Create New Network** (Créer un nouvel objet réseau) pour créer l'objet maintenant.

Le graphique suivant montre à quoi la première étape doit ressembler.



d) Définissez la configuration de confidentialité, puis cliquez sur **Next** (Suivant).

- **Politique IKE** : les paramètres IKE n'ont aucune incidence sur le hairpinning. Sélectionnez simplement les versions, les politiques et les propositions IKE qui correspondent à vos besoins de sécurité. Notez les clés prépartagées locales et distantes que vous saisissez : vous en aurez besoin lors de la configuration de l'homologue distant.
- **Exemption**de NAT : sélectionnez l'interface interne.



- **Diffie Hellman Group for Perfect Forward Secrecy** (Groupe Diffie Hellman pour la confidentialité persistante) : ce paramètre n'a aucune incidence sur le hairpinning. Configurez-le comme bon vous semble.

e) Cliquez sur **Terminer**.

Le résumé de la connexion est copié dans le presse-papiers. Vous pouvez le coller dans un fichier texte ou tout autre document pour vous aider à configurer l'homologue distant.

Étape 2 (Site A, site principal.) Configurez la règle NAT pour traduire toutes les connexions sortant de l'interface externe en ports sur l'adresse IP externe (PAT de l'interface).

Lorsque vous avez terminé la configuration initiale du périphérique, le système crée une règle NAT nommée InsideOutsideNatRule. Cette règle applique la PAT d'interface au trafic IPv4 de toute interface qui quitte le périphérique par l'intermédiaire de l'interface externe. Comme l'interface externe est incluse dans l'interface source « Any », la règle dont vous avez besoin existe déjà, sauf si vous l'avez modifiée ou supprimée.

La procédure suivante explique comment créer la règle dont vous avez besoin.

a) Cliquez sur **Policies (Politiques)** > **NAT**.
b) Effectuez l'une des opérations suivantes :

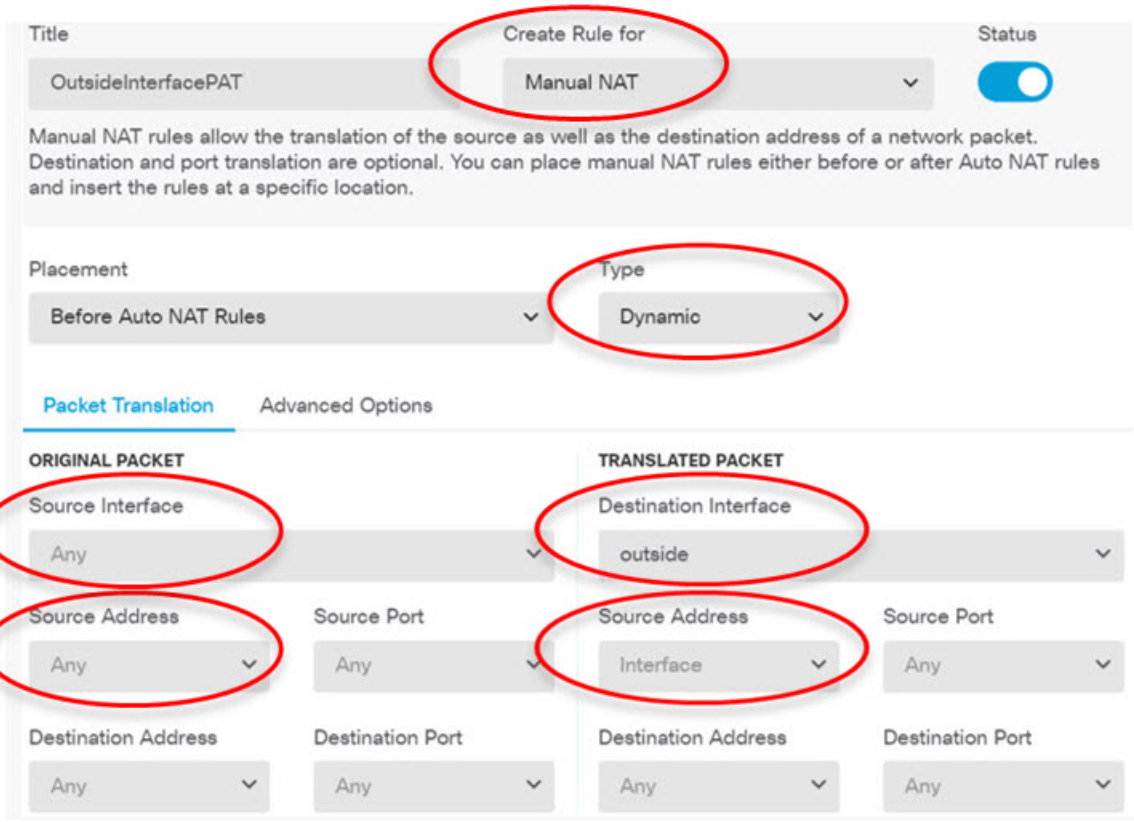
- Pour modifier la règle InsideOutsideNatRule, passez le curseur sur la colonne **Action** et cliquez sur l'icône de modification ( ).
- Pour créer une nouvelle règle, cliquez sur le bouton **+**.

c) Configurez une règle avec les propriétés suivantes :

- **Title** (Titre) : pour une nouvelle règle, saisissez un nom significatif, sans espaces. Par exemple, OutsideInterfacePAT.
- **Create Rule For** (Créer une règle pour) : **Manual NAT** (NAT manuelle).
- **Placement** : **Before Auto NAT Rules (Avant les règles de NAT automatique)** (valeur par défaut).
- **Type** :**Dynamic** (Dynamique).
- **Original Packet** (Paquet d'origine) : pour **Source Address** (Adresse source), sélectionnez Any (tout) ou any-ipv4. Pour **Source Interface** (Interface source), veillez à sélectionner Any (tout) (qui est la valeur par défaut). Pour toutes les autres options de Original Packet (Paquet d'origine), conservez la valeur par défaut, Any (tout).

- **Translated Packet** (Paquet traduit) : pour **Destination Interface** (Interface de destination), sélectionnez externe. Pour **Translated Address** (Adresse traduite), sélectionnez **Interface**. Pour toutes les autres options de Translated Packet (Paquet traduit), conservez la valeur par défaut, Any (tout).

Le graphique suivant montre le cas simple où vous sélectionnez Any (tout) pour l'adresse source.



d) Cliquez sur **OK**.

Étape 3 (Site A, site principal.) Configurez une règle de contrôle d'accès pour autoriser l'accès au réseau protégé sur le site B.

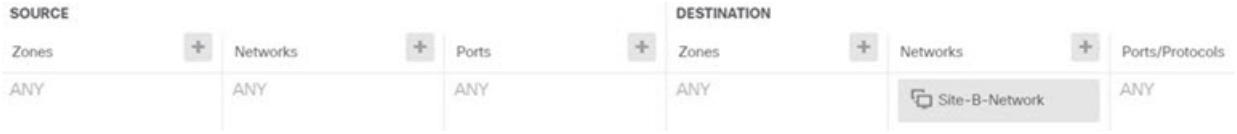
La simple création d'une connexion VPN n'autorise pas automatiquement le trafic sur le VPN. Vous devez vous assurer que votre stratégie de contrôle d'accès autorise le trafic vers le réseau distant.

La procédure suivante montre comment ajouter une règle spécifiquement pour le réseau distant. Le fait que vous ayez besoin d'une règle supplémentaire dépend de vos règles existantes.

a) Cliquez sur **Policies (Politiques)** > **Access Control (Contrôle d'accès)**.
b) Cliquez sur + pour créer une nouvelle règle.
c) Configurez une règle avec les propriétés suivantes :

- **Order** (Ordre) : sélectionnez une position dans la politique avant toute autre règle qui pourrait correspondre à ces connexions et les bloquer. La valeur par défaut consiste à ajouter la règle à la fin de la politique. Si vous devez repositionner la règle ultérieurement, vous pouvez modifier cette option ou simplement faire glisser et déposer la règle dans le bon emplacement dans le tableau.
- **Titre** : saisissez un nom significatif sans espaces. Par exemple, Site-B-Network.

- **Action** : **Autoriser**. Vous pouvez sélectionner Trust (Confiance) si vous ne souhaitez pas que ce trafic soit inspecté pour détecter des violations de protocole ou des intrusions.
- Onglet **Source/Destination** : pour **Destination** > **Network (Réseau)**, sélectionnez le même objet que vous avez utilisé dans le profil de connexion VPN pour le réseau distant. Laissez la valeur par défaut, Any, (tout), pour toutes les autres options de source et de destination.



- Onglets **Application**, **URL** et **Users** (Utilisateurs) : laissez les paramètres par défaut sur ces onglets, c'est-à-dire qu'aucune option n'est sélectionnée.
- Onglets **Intrusion**, **File** (Fichiers) : vous pouvez, au besoin, sélectionner des politiques de prévention des intrusions ou des politiques de fichiers afin d'inspecter les menaces ou les logiciels malveillants.
- Onglet**Logging (journalisation**) : vous pouvez éventuellement activer la journalisation des connexions.

d) Cliquez sur **OK**.

Étape 4 (Site A, site principal.) Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement. Si vous laissez la fenêtre ouverte, elle indiquera qu'il n'y a aucune modification en attente après un déploiement réussi.

Étape 5 (Site B, site distant.) Connectez-vous au périphérique du site distant et configurez la connexion VPN de site à site pour le site A.

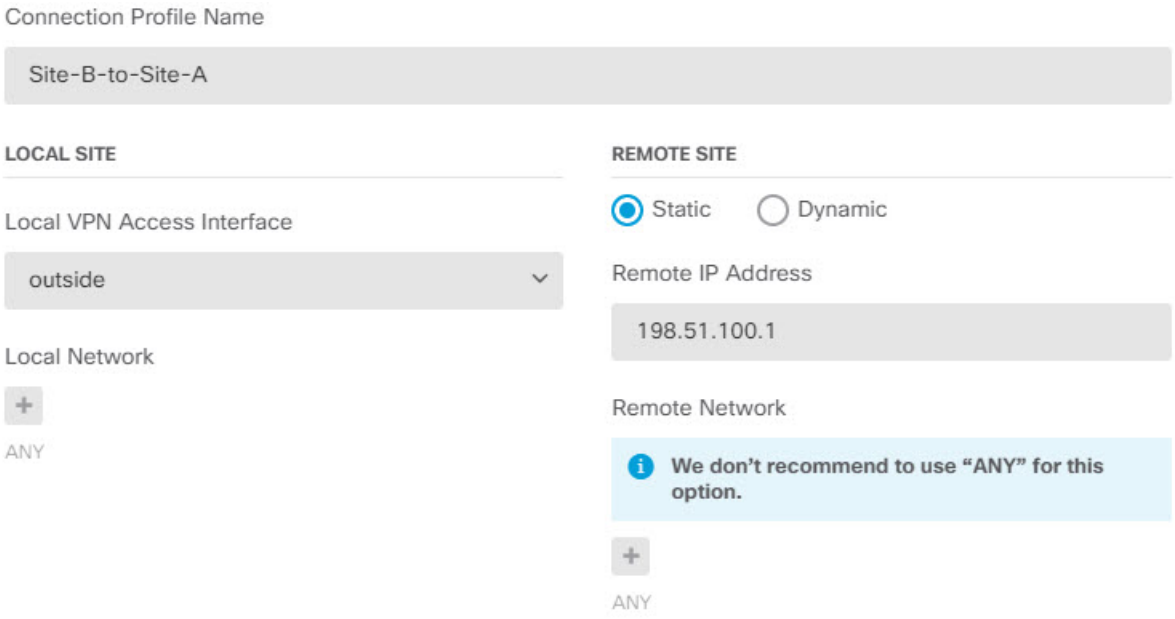
Utilisez le résumé de connexion obtenu à partir de la configuration du périphérique du site A pour vous aider à configurer le côté du site B de la connexion.

a) Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le groupe Connexion VPN de site à site.
b) Cliquez sur **+** pour ajouter une nouvelle connexion.
c) Définissez les points terminaux comme suit, puis cliquez sur **Next** (Suivant) :

- **Connection Profile Name** (Nom du profil de connexion) : donnez à la connexion un nom significatif, par exemple Site-B-vers-Site-A.
- **Local VPN Access Interface** (Interface d'accès VPN locale) : sélectionnez l'interface externe.
- **Local Network** (Réseau local) : cliquez sur **+**, puis sélectionnez l'objet réseau qui définit le réseau protégé local. Dans cet exemple, 192.168.2.0/24. Vous pouvez cliquer sur **Create New Network** (Créer un nouvel objet réseau) pour créer l'objet maintenant.

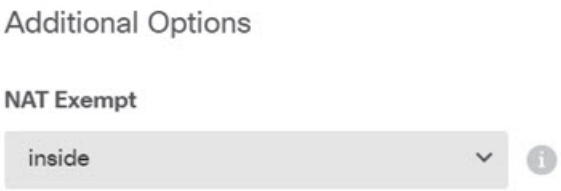
- **Remote IP Address** (Adresse IP distante) : saisissez l'adresse IP de l'interface externe du site principal. Dans cet exemple, 198.51.100.1.
- **distant Network** (Réseau distant) : conservez la valeur par défaut, Any (Tout). Ignorez l'avertissement ; il n'est pas pertinent pour ce scénario d'utilisation.

Le graphique suivant montre à quoi la première étape doit ressembler.



d) Définissez la configuration de confidentialité, puis cliquez sur **Next** (Suivant).

- **Politique IKE** : les paramètres IKE n'ont aucune incidence sur le hairpinning. Configurez les mêmes options ou des options compatibles que celles de la fin de la connexion VPN du site A. Vous devez configurer correctement les clés prépartagées : inversez les clés locales et distantes (pour IKEv2) comme configuré sur le périphérique du site A. Pour IKEv1, il n'y a qu'une seule clé, qui doit être la même sur les deux homologues.
- **NAT Exempt** (Exemption NAT) : sélectionnez l'interface interne.



- **Diffie Hellman Group for Perfect Forward Secrecy** (Groupe Diffie Hellman pour la confidentialité persistante) : ce paramètre n'a aucune incidence sur le hairpinning. Faire correspondre le paramètre utilisé à la fin de la connexion VPN du site A.

e) Cliquez sur **Terminer**.

Étape 6 (Site B, site distant.) Supprimez toutes les règles NAT pour le réseau protégé afin que tout le trafic sortant du site doive passer par le tunnel VPN.

L'exécution de la NAT sur ce périphérique est inutile, car c'est le périphérique du site A qui effectuera la traduction d'adresses. Mais veuillez examiner votre situation spécifique. Si vous avez plusieurs réseaux internes et qu'ils ne prennent pas tous part à cette connexion VPN, ne supprimez pas les règles NAT dont vous avez besoin pour ces réseaux.

a) Cliquez sur **Policies (Politiques)** > **NAT**.
b) Effectuez l'une des opérations suivantes :

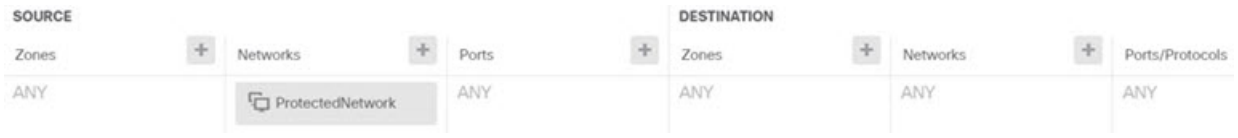
- Pour supprimer des règles, passez le curseur sur la colonne Action et cliquez sur l'icône de suppression ( ).
- Pour modifier les règles afin qu'elles ne s'appliquent plus au réseau protégé, passez le curseur sur la colonne Action et cliquez sur l'icône de modification ( ).

Étape 7 (Site B, site distant.) Configurez une règle de contrôle d'accès pour autoriser l'accès du réseau protégé à Internet.

L'exemple suivant permet le trafic du réseau protégé vers n'importe quelle destination. Vous pouvez l'ajuster selon vos besoins précis. Vous pouvez également faire précéder la règle de règles de blocage pour filtrer le trafic indésirable. Une autre option consiste à configurer les règles de blocage sur l'appareil du site A.

a) Cliquez sur **Policies (Politiques)** > **Access Control (Contrôle d'accès)**.
b) Cliquez sur **+** pour créer une nouvelle règle.
c) Configurez une règle avec les propriétés suivantes :

- **Order** (Ordre) : sélectionnez une position dans la politique avant toute autre règle qui pourrait correspondre à ces connexions et les bloquer. La valeur par défaut consiste à ajouter la règle à la fin de la politique. Si vous devez repositionner la règle ultérieurement, vous pouvez modifier cette option ou simplement faire glisser et déposer la règle dans le bon emplacement dans le tableau.
- **Titre** : saisissez un nom significatif sans espaces. Par exemple, Protected-Network-to-Any.
- **Action** : **Autoriser**. Vous pouvez sélectionner Trust (Confiance) si vous ne souhaitez pas que ce trafic soit inspecté pour détecter des violations de protocole ou des intrusions.
- Onglet **Source/Destination** : pour **Source** > **Network (Réseau)**, sélectionnez le même objet que vous avez utilisé dans le profil de connexion VPN pour le réseau local. Laissez la valeur par défaut, Any, (tout), pour toutes les autres options de source et de destination.



- Onglets **Application**, **URL** et **Users** (Utilisateurs) : laissez les paramètres par défaut sur ces onglets, c'est-à-dire qu'aucune option n'est sélectionnée.
- Onglets **Intrusion**, **File** (Fichiers) : vous pouvez, au besoin, sélectionner des politiques de prévention des intrusions ou des politiques de fichiers afin d'inspecter les menaces ou les logiciels malveillants.
- Onglet**Logging (journalisation**) : vous pouvez éventuellement activer la journalisation des connexions.

d) Cliquez sur **OK**.

Étape 8 (Site B, site distant.) Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant) et attendez la fin du déploiement.

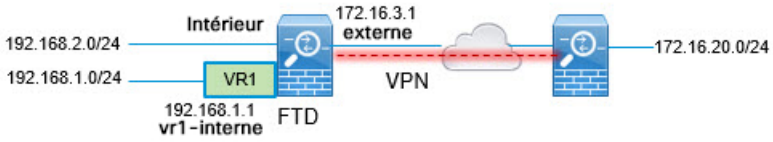
Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement. Si vous laissez la fenêtre ouverte, elle indiquera qu'il n'y a aucune modification en attente après un déploiement réussi.

Sécuriser le trafic de réseaux dans plusieurs routeurs virtuels sur un VPN de site à site

Si vous configurez plusieurs routeurs virtuels sur un périphérique, vous devez configurer le VPN de site à site dans le routeur virtuel global. Vous ne pouvez pas configurer le VPN de site à site sur une interface affectée à un routeur virtuel personnalisé.

Comme les tables de routage pour les routeurs virtuels sont distinctes, vous devez créer des routes statiques si vous devez sécuriser les connexions des réseaux hébergés dans des routeurs virtuels personnalisés sur le VPN de site à site. Vous devez également mettre à jour la connexion VPN de site à site pour inclure ces réseaux supplémentaires.

Prenons l'exemple suivant. Dans ce cas, le VPN de site à site est défini sur l'interface externe à l'adresse 172.16.3.1. Ce VPN peut inclure le réseau interne 192.168.2.0/24 sans configuration supplémentaire, car l'interface interne fait également partie du routeur virtuel global. Mais, pour fournir des services VPN de site à site au réseau 192.168.1.0/24, qui fait partie du routeur virtuel VR1, vous devez configurer des routes statiques dans les deux sens, et ajouter le réseau à la configuration VPN de site à site.



Avant de commencer

Cet exemple suppose que vous ayez déjà configuré le VPN de site à site entre le réseau local 192.168.2.0/24 et le réseau externe 172.16.20.0/24, défini les routeurs virtuels et configuré et affecté les interfaces aux routeurs virtuels appropriés.

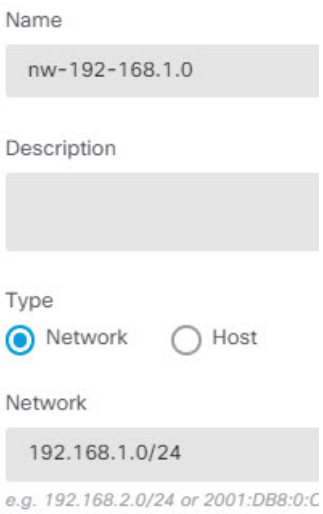
Procédure

Étape 1 Configurez la fuite de route du routeur virtuel global vers VR1.

Cette fuite de route permet aux points terminaux protégés par l'extrémité externe (distant) du VPN de site à site d'accéder au réseau 192.168.1.0/24 dans le routeur virtuel VR1.

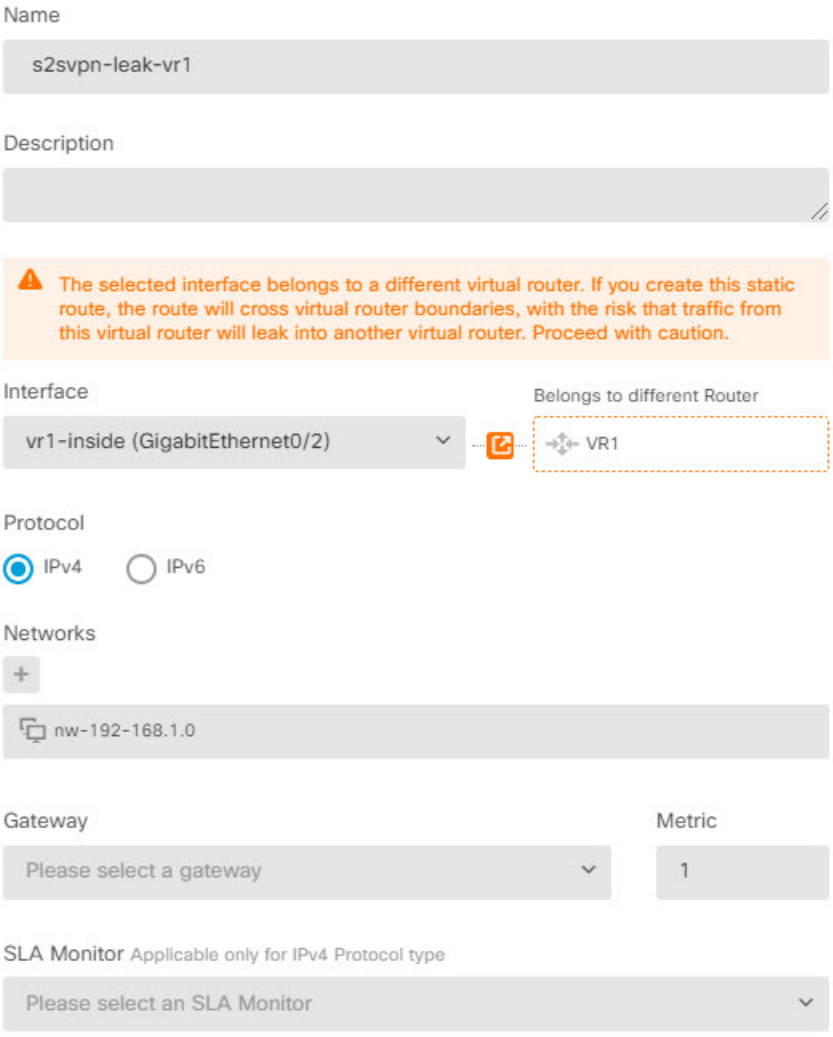
a) Choisissez **Device (Périphérique)** > **Routing (Routage)** > **View Configuration (Afficher la configuration)**.
b) Cliquez sur l'icône d'affichage ( ) du routeur virtuel global.
c) Dans l'onglet **Static Routing** (Routage statique) du routeur virtuel global, cliquez sur **+** et configurez la route :

- **Nom** : n'importe quel nom suffit, tel que **s2svpn-leak-vr1**.
- **Interface** : sélectionnez **vr1-inside**.
- **Protocole** : sélectionnez **IPv4**.
- **Réseaux** : sélectionnez un objet qui définit le réseau 192.168.1.0/24. Cliquez sur **Create New Network** (Créer un nouveau réseau) pour créer l'objet maintenant, si nécessaire.



- **Gateway** (passerelle) : laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



d) Cliquez sur **OK**.

Étape 2 Configurez la fuite de route de VR1 vers le routeur virtuel global :

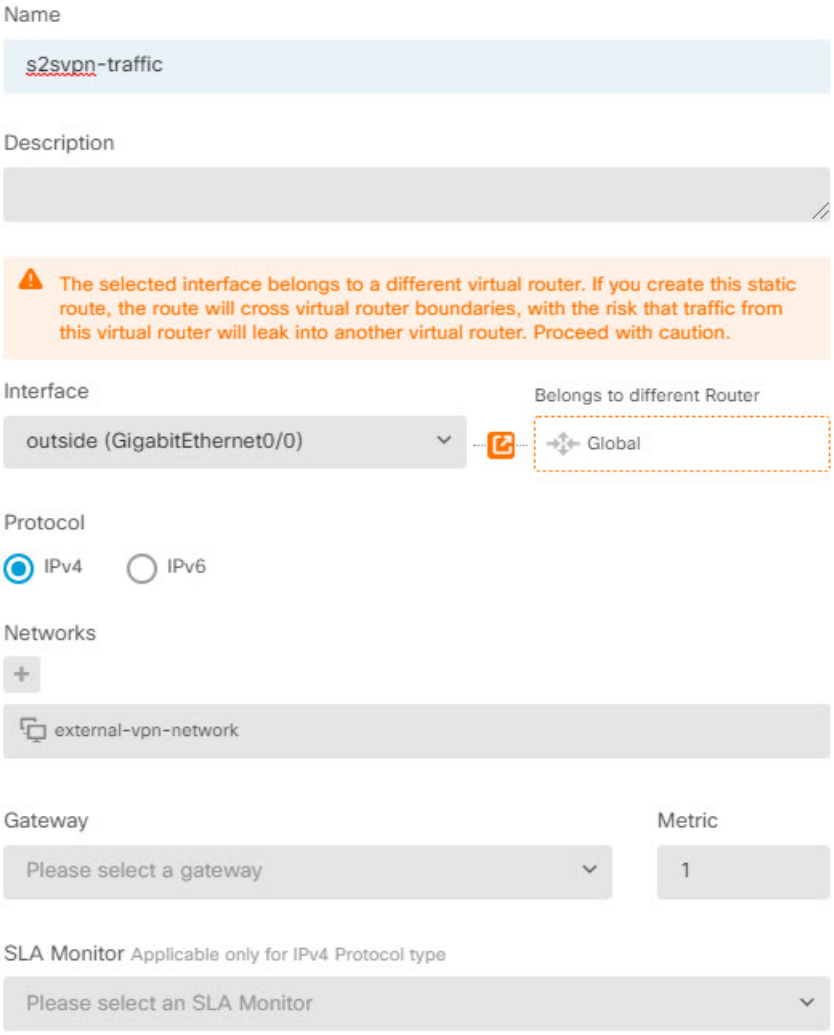
Cette route permet aux points terminaux sur le réseau 192.168.1.0/24 d'établir des connexions qui traverseront le tunnel VPN de site à site. Pour cet exemple, le point terminal distant protège le réseau 172.16.20.0/24.

a) Choisissez **VR1** dans la liste déroulante des routeurs virtuels pour passer à la configuration VR1.
b) Dans l'onglet **Static Routing** (Routage statique) du routeur virtuel VR1, cliquez sur + et configurezla route :

- **Nom** : n'importe quel nom suffit, tel que **s2svpn-traffic**.
- **Interface** : sélectionnez **outside**.
- **Protocole** : sélectionnez **IPv4**.
- **Réseaux** : sélectionnez l'objet que vous avez créé pour les réseaux protégés du point terminal distant, par exemple, **externe-vpn-network**.

- **Gateway** (passerelle) : laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



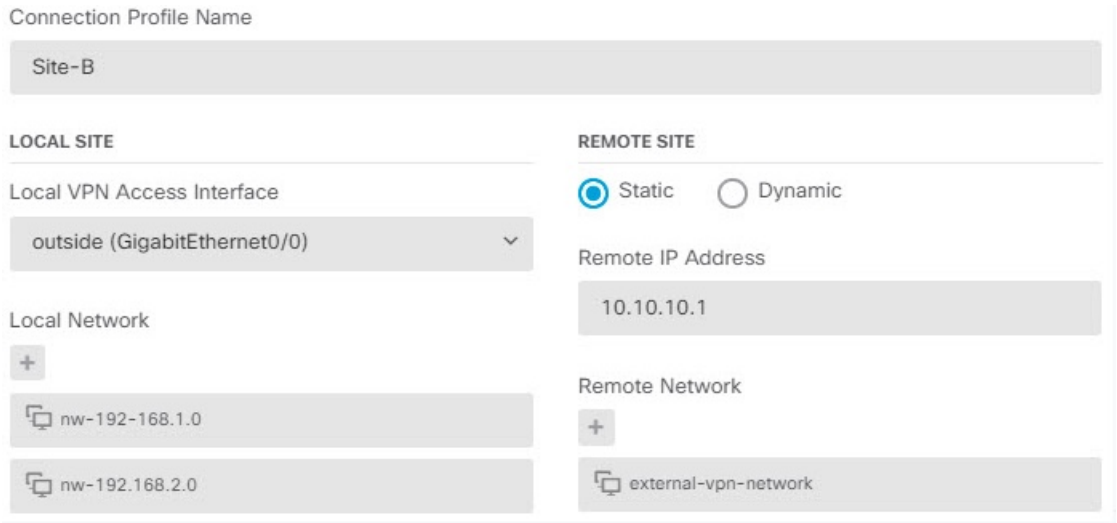
c) Cliquez sur **OK**.

Étape 3 Ajoutez le réseau 192.168.1.0/24 au profil de connexion VPN de site à site :

a) Choisissez **Device (Périphérique)** > **Site-to-Site VPN (VPN de site à site)** > **View Configuration (Afficher la configuration)**.

b) Cliquez sur l'icône de modification ( ) du profil de connexion.

c) Sur la première page de l'assistant, cliquez sur **+** sous **Local Network (Réseau local)**, puis ajoutez l'objet correspondant au réseau 192.168.1.0/24.



d) Achevez l'assistant.



CHAPITRE 25

VPN d'accès à distance

Le réseau privé virtuel (VPN) d'accès à distance permet aux utilisateurs individuels de se connecter à votre réseau à partir d'un emplacement distant à l'aide d'un ordinateur ou d'autres périphériques pris en charge connectés à Internet. Cela permet aux collaborateurs mobiles de se connecter à partir de leur réseau domestique ou d'un réseau Wi-Fi public, par exemple.

Les rubriques suivantes expliquent comment configurer le VPN d'accès à distance pour votre réseau.

- Aperçu du VPN d'accès à distance, à la page 703
- Exigences de licence pour le VPN d'accès à distance, à la page 710
- Consignes et limites pour le VPN d'accès à distance, à la page 710
- Configuration du VPN d'accès à distance, à la page 711
- Gestion de la configuration VPN d'accès à distance, à la page 718
- Surveillance du VPN d'accès à distance, à la page 733
- Dépannage des VPN d'accès à distance, à la page 733
- Exemples d'utilisation du VPN d'accès à distance, à la page 736

Aperçu du VPN d'accès à distance

Vous pouvez utiliser Gestionnaire de périphériques de pare-feu pour configurer le VPN d'accès à distance sur SSL à l'aide du logiciel client AnyConnect.

Lorsque le client AnyConnect client négocie une connexion SSL VPN avec le Firewall Threat Defense périphérique, il se connecte à l'aide de Transport Layer Security (TLS) ou de Datagram Transport Layer Security (DTLS). L'utilisation de DTLS évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets. Le client et le périphérique Firewall Threat Defense négocient la version TLS/DTLS à utiliser. DTLS est utilisé si le client le prend en charge.

Nombre maximal de sessions VPN simultanées par modèle de périphérique

Il y a une limite maximale au nombre de sessions VPN simultanées autorisées sur un périphérique selon son modèle. Cette limite est conçue pour que les performances du système ne se dégradent pas à des niveaux inacceptables. La limite est une combinaison des utilisateurs de VPN d'accès à distance et des homologues de VPN de site à site. Utilisez ces limites pour la planification de la capacité.

Modèle du périphérique	Nombre maximal de sessions VPN simultanées
ASA 5508-X	100
ASA 5516-X	300
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower de la série 2110	1 500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10 000
Firepower 4100, tous les modèles	10 000
Appareils Cisco Firepower de série 9300, tous les modèles	20 000
FTDv: FTDv5	50
FTDv: FTDv10, FTDv20, FTDv30	250
FTDv: FTDv50	750
FTDv: FTDv100	10 000
ISA 3000	25

Téléchargement du logiciel client AnyConnect

Avant de pouvoir configurer un VPN d'accès à distance, vous devez télécharger le logiciel client AnyConnect sur votre ordinateur. Vous devrez charger ces paquets lors de la définition du VPN.

Vous devez télécharger la dernière version client AnyConnect pour vous assurer de disposer des dernières fonctionnalités, des corrections de bogues et des correctifs de sécurité. Mettez régulièrement à jour les paquets sur le périphérique Firepower Threat Defense.



Remarque Vous pouvez charger un paquet client AnyConnect par système d'exploitation : Windows, Mac et Linux. Vous ne pouvez pas charger plusieurs versions pour un type de système d'exploitation donné.

Obtenez les paquets de logiciels client AnyConnect depuis software.cisco.com. Vous devez télécharger les versions « Full Installation Package » (ensemble d'installation comple) des clients.

Comment les utilisateurs peuvent installer le logiciel client AnyConnect

Pour établir une connexion VPN, vos utilisateurs doivent installer le logiciel client AnyConnect. Vous pouvez utiliser vos méthodes de distribution de logiciels existantes pour installer le logiciel directement. Vous pouvez également faire en sorte que les utilisateurs installent client AnyConnect directement à partir du périphérique Firewall Threat Defense.

Les utilisateurs doivent avoir des droits d'administrateur sur leur poste de travail pour installer le logiciel.

Une fois le client AnyConnect installé, si vous chargez de nouvelles versions client AnyConnect sur le système, le client AnyConnect détectera la nouvelle version lors de la prochaine connexion VPN effectuée par l'utilisateur. Le système invitera automatiquement l'utilisateur à télécharger et à installer le logiciel client mis à jour. Cette automatisation simplifie la distribution des logiciels pour vous et vos clients.

Si vous décidez que les utilisateurs installent initialement le logiciel à partir du périphérique Firewall Threat Defense, demandez aux utilisateurs de procéder comme suit.

Remarque Les utilisateurs d'Android et d'iOS doivent télécharger client AnyConnect à partir de l'App Store approprié.

Procédure

Étape 1 À l'aide d'un navigateur Web, ouvrez **https://***ravpn-address*, où *ravpn-address* est l'adresse IP ou le nom d'hôte de l'interface externe sur laquelle vous autorisez les connexions VPN.

Vous identifiez cette interface lorsque vous configurez le VPN d'accès à distance. Le système invite l'utilisateur à se connecter.

Si vous avez modifié le port pour les connexions VPN d'accès à distance, les utilisateurs doivent inclure le port personnalisé dans l'URL. Par exemple : si vous avez changé le port en 4443 : https://ravpn.example.com:4443

Étape 2 Connectez-vous au site.

Les utilisateurs sont authentifiés à l'aide du serveur de répertoire configuré pour le VPN d'accès à distance. La connexion doit être réussie pour continuer.

Si la connexion a réussi, le système détermine si l'utilisateur dispose déjà de la version requise de client AnyConnect. Si client AnyConnect est absent de l'ordinateur de l'utilisateur ou s'il est de niveau inférieur, le système commence automatiquement l'installation du logiciel client AnyConnect.

Lorsque l'installation est terminée, client AnyConnect termine la connexion VPN d'accès à distance.

Contrôle des autorisations et des attributs des utilisateurs à l'aide de RADIUS et des stratégies de groupe

Vous pouvez appliquer des attributs d'autorisation d'utilisateur (également appelés droits ou autorisations d'utilisateur) aux connexions VPN RA à partir d'un serveur RADIUS externe ou d'une politique de groupe définie sur le périphérique Firepower Threat Defense. Si le périphérique Firepower Threat Defense reçoit des

attributs du serveur AAA externe qui sont en conflit avec ceux configurés dans la politique de groupe, les attributs du serveur AAA prévalent toujours.

Le périphérique Firepower Threat Defense applique les attributs dans l'ordre suivant :

1. Attributs de l'utilisateur sur le serveur AAA externe : le serveur renvoie ces attributs une fois l'authentification ou l'autorisation de l'utilisateur réussie.
2. Politique de groupe configurée sur le périphérique Firepower Threat Defense : si un serveur RADIUS renvoie la valeur de l'attribut de classe RADIUS IETF-Class-25 (OU= group-policy) pour l'utilisateur, le périphérique place l'utilisateur dans la politique de groupe du même nom et applique les attributs de la politique de groupe qui ne sont pas renvoyés par le serveur.Firepower Threat Defense
3. Politiques de groupe affectées par le profil de connexion (également appelé groupes de tunnels) : le profil de connexion contient les paramètres préliminaires pour la connexion et comprend une politique de groupe par défaut appliquée à l'utilisateur avant l'authentification. Tous les utilisateurs se connectant au périphérique Firepower Threat Defense appartiennent initialement à ce groupe, qui fournit tous les attributs manquants dans les attributs d'utilisateur renvoyés par le serveur AAA ou dans la politique de groupe attribuée à l'utilisateur.

Les périphériques FTD prennent en charge les attributs avec l'ID de fournisseur 3076. Si le serveur RADIUS que vous utilisez ne comporte pas ces attributs définis, vous devez les définir manuellement. Pour définir un attribut, utilisez le nom ou le numéro d'attribut, le type, la valeur et le code du fournisseur (3076).

Les rubriques suivantes expliquent les attributs pris en charge selon que les valeurs sont définies dans le serveur RADIUS ou s'il s'agit de valeurs que le système envoie au serveur RADIUS.

Attributs envoyés au serveur RADIUS

Les attributs RADIUS 146 et 150 sont envoyés du périphérique Firepower Threat Defense au serveur RADIUS pour les demandes d'authentification et d'autorisation. Tous les attributs suivants sont envoyés du périphérique Firepower Threat Defense au serveur RADIUS pour les demandes de démarrage, de mise à jour provisoire et d'arrêt de gestion.

Tableau 15 : Attributs Firewall Threat Defense envoyés à RADIUS

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Type de client	150	nombre entier	Unique	Le type de client qui se connecte au VPN : 2 = client AnyConnect VPN SSL
Type de séance	151	nombre entier	Unique	Le type de connexion : 1 = client AnyConnect VPN SSL
Tunnel Group Name	146	Chaîne	Unique	Le nom du profil de connexion qui a été utilisé pour établir la session, tel qu'il est défini sur le périphérique Firepower Threat Defense. Ce nom peut comporter de 1 à 253 caractères.

Attributs reçus du serveur RADIUS

Les attributs d'autorisation utilisateur suivants sont envoyés au périphérique Firepower Threat Defense par le serveur RADIUS.

Tableau 16 : Attributs RADIUS envoyés à Firewall Threat Defense

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Liste d'accès entrant	86	Chaîne	Unique	Les deux attributs Access-List (Liste d'accès) prennent le nom d'une ACL configurée sur le périphérique Firepower Threat Defense. Créez ces ACLs en utilisant le type d'objet Smart CLI Extended Access List (liste d'accès étendue Smart CLI) (sélectionnez **Device (périphérique)** > **Advanced Configuration (configuration avancée)** > **Smart CLI** > **Objects (objets)**). Ces listes de contrôle d'accès contrôlent le flux du trafic dans le sens entrant (trafic entrant sur le périphérique Firepower Threat Defense) ou sortant (trafic sortant du périphérique Firepower Threat Defense.
Liste d'accès sortante	87	Chaîne	Unique	
Ensembles des adresses	217	Chaîne	Unique	Le nom d'un objet réseau défini sur le périphérique Firepower Threat Defense qui identifie un sous-réseau, qui sera utilisé comme groupement d'adresses pour les clients se connectant au VPN d'accès à distance. Définissez l'objet réseau dans la page **Objects** (objets).
Banner1	15	Chaîne	Unique	Bannière à afficher lorsque l'utilisateur se connecte.
Banner2	36	Chaîne	Unique	La deuxième partie de la bannière à afficher lorsque l'utilisateur se connecte. Bannière2 est ajouté à Bannière1.
Politique de groupe	25	Chaîne	Unique	La politique de groupe à utiliser dans la connexion. Vous devez créer la politique de groupe sur la page **Group Policy** (politique de groupe) du VPN d'accès à distance. 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*;
Connexions simultanées	2	nombre entier	Unique	Nombre de connexions simultanées distinctes que l'utilisateur est autorisé à établir, 0 à 2147483647.
VLAN	140	nombre entier	Unique	Le VLAN dans lequel limiter la connexion de l'utilisateur, 0 à 4094. Vous devez également configurer ce VLAN sur une sous-interface du périphérique Firepower Threat Defense.

Authentification à deux facteurs

Vous pouvez configurer l'authentification à deux facteurs pour le VPN RA. Avec l'authentification à deux facteurs, l'utilisateur doit fournir un nom d'utilisateur et un mot de passe statiques, ainsi qu'un élément supplémentaire comme un jeton RSA ou un code d'accès Duo. L'authentification à deux facteurs diffère de l'utilisation d'une deuxième source d'authentification en ce sens que l'authentification à deux facteurs est configurée sur une source d'authentification unique, la relation avec le serveur RSA/Duo étant liée à la source d'authentification principale. L'exception est Duo LDAP, où vous configurez le serveur LDAP Duo comme source d'authentification secondaire.

Le système a été testé avec des jetons RSA et des codes d'accès Duo envoyés à Duo Mobile pour le deuxième facteur, conjointement avec tout serveur RADIUS ou AD comme premier facteur dans le processus d'authentification à deux facteurs.

Authentification à deux facteurs RSA

Vous pouvez configurer RSA en utilisant l'une des approches suivantes. Consultez la documentation de RSA pour obtenir des renseignements sur la configuration côté RSA.

- Définissez le serveur RSA directement dans Gestionnaire de périphériques de pare-feu en tant que serveur RADIUS, et utilisez ce serveur comme source d'authentification principale dans le VPN d'accès à distance.

  Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré sur le serveur RADIUS RSA, puis concaténer le mot de passe avec le jeton RSA temporaire à usage unique, en séparant le mot de passe et le jeton par une virgule : *password*,*token*.

  Dans cette configuration, il est courant d'utiliser un serveur RADIUS distinct (comme celui fourni dans Cisco ISE) pour fournir les services d'autorisation. Vous devez configurer le deuxième serveur RADIUS en tant qu'autorisation et, éventuellement, serveur de comptabilité.

- Intégrer le serveur RSA avec un serveur RADIUS ou AD qui prend en charge l'intégration directe, et configurer le VPN d'accès à distance pour utiliser le serveur RADIUS ou AD non RSA comme source d'authentification principale. Dans ce cas, le serveur RADIUS/AD utilise RSA-SDI pour déléguer et orchestrer l'authentification à deux facteurs entre le client et le serveur RSA.

  Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré sur le serveur RADIUS ou AD, et concaténer le mot de passe avec le jeton RSA à usage unique temporaire, en séparant le mot de passe et le jeton par une virgule : *password*,*token*.

  Dans cette configuration, vous utilisez également le serveur RADIUS non RSA comme serveur d'autorisation et, éventuellement, serveur de comptabilité.

Authentification à deux facteurs Duo au moyen de RADIUS

Vous pouvez configurer le serveur RADIUS Duo comme source d'authentification principale. Cette approche utilise le serveur mandataire d'authentification RADIUS Duo.

Pour les étapes détaillées de la configuration de Duo, consultez https://duo.com/docs/cisco-firepower.

Vous devez ensuite configurer Duo pour transférer les demandes d'authentification dirigées vers le serveur mandataire pour utiliser un autre serveur RADIUS, ou un serveur AD, comme premier facteur d'authentification et le service en nuage Duo comme deuxième facteur.

Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré sur le mandataire d'authentification Duo et le serveur RADIUS/AD associé, et le mot de passe pour le nom d'utilisateur configuré dans le serveur RADIUS/AD, suivi de l'un des codes Duo suivants :

- *Duo-passcode*. Par exemple, *my-password*,**12345**.
- **push**. Par exemple, *mon-motdepasse*,**push**. Utilisez **push** pour demander à Duo d'envoyer une authentification push à l'application Duo Mobile, que l'utilisateur doit déjà avoir installée et enregistrée.
- **sms**. Par exemple, *mon-motdepasse*,**sms**. Utilisez **sms** pour demander à Duo d'envoyer un message SMS avec un nouveau lot de codes d'authentification au périphérique mobile de l'utilisateur. La tentative d'authentification de l'utilisateur échouera lors de l'utilisation de **sms**. L'utilisateur doit ensuite s'authentifier de nouveau et saisir le nouveau mot de passe comme facteur secondaire.
- **phone**. Par exemple, *mon-motdepasse*,**phone**. Utilisez **phone** pour demander à Duo d'effectuer l'authentification par rappel téléphonique.

Si le nom d'utilisateur/mot de passe est authentifié, le mandataire d'authentification Duo contacte le service en nuage Duo, qui valide que la demande provient d'un appareil mandataire configuré valide, puis envoie un code d'accès temporaire au périphérique mobile de l'utilisateur, comme indiqué. Lorsque l'utilisateur accepte ce code d'accès, la session est marquée comme authentifiée par Duo et le VPN d'accès à distance est établi.

Authentification à deux facteurs Duo avec LDAP

Vous pouvez utiliser le serveur LDAP Duo comme source d'authentification secondaire en conjonction avec un serveur Microsoft Active Directory (AD) ou RADIUS comme source principale. Avec Duo LDAP, l'authentification secondaire valide l'authentification principale avec un code d'accès Duo, une notification poussée ou un appel téléphonique.

Le périphérique Firepower Threat Defense communique avec Duo LDAP à l'aide de LDAPS sur le port TCP/636.

Notez que le serveur LDAP Duo fournit des services d'authentification uniquement, il ne fournit pas de services d'identité. Ainsi, si vous utilisez Duo LDAP comme source d'authentification principale, vous ne verrez pas les noms d'utilisateurs associés aux connexions VPN d'accès à distance dans les tableaux de bord, et vous ne pourrez pas écrire de règles de contrôle d'accès pour ces utilisateurs.

Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré à la fois sur le serveur RADIUS/AD et sur le serveur LDAP Duo. Lorsqu'il est invité à se connecter par le client AnyConnect, l'utilisateur fournit le mot de passe RADIUS/AD dans le champ **Password** (Mot de passe) principal et, dans **Secondary Password** (Mot de passe secondaire), fournit l'un des éléments suivants pour s'authentifier auprès de Duo. Pour en savoir plus, consultez https://guide.duo.com/anyconnect.

- *Duo passcode* (Code d'accès Duo) : authentifiez-vous à l'aide d'un code d'accès, généré avec Duo Mobile, envoyé par SMS, généré par votre jeton matériel ou fourni par un administrateur. Par exemple, 1234567.
- **push** (Notification poussée) : envoyez une demande de connexion à votre téléphone, si vous avez installé et activé l'application Duo Mobile. Passez en revue la demande et appuyez sur **Approve** (Approuver) pour vous connecter.
- **Téléphone** : authentifiez-vous à l'aide d'un rappel téléphonique.
- **SMS** : demandez un code d'accès Duo dans un message texte. La tentative de connexion échouera. Connectez-vous à nouveau en utilisant le nouveau code d'accès.

Pour une explication détaillée et un exemple d'utilisation de Duo LDAP, consultez Comment configurer l'authentification à deux facteurs à l'aide de Duo LDAP, à la page 745.

Exigences de licence pour le VPN d'accès à distance

Votre licence de périphérique de base doit respecter les exigences d'exportation avant que vous puissiez configurer le VPN d'accès à distance. Lorsque vous enregistrez le périphérique, vous devez le faire avec un compte Smart Software Manager qui est activé pour les fonctionnalités d'exportation contrôlée. Vous ne pouvez pas non plus configurer la fonctionnalité à l'aide de la licence d'évaluation.

En outre, vous devez acheter et activer une licence VPN d'accès à distance, l'une des licences suivantes : AnyConnect Plus, AnyConnect Apex, ou VPN AnyConnect . Ces licences sont traitées de la même manière pour les périphériques Firewall Threat Defense, même si elles sont conçues pour permettre différents ensembles de fonctionnalités lorsqu'elles sont utilisées avec des têtes de réseau ASA basées sur le logiciel.

Pour activer la licence, sélectionnez **Device (Périphérique)** > **Smart License (Licence Smart)** > **View Configuration (Afficher la configuration)**, puis sélectionnez la licence appropriée dans le groupe de licences RA VPN License (Licence VPN RA). La licence doit être disponible dans votre compte Smart Software Manager. Pour en savoir plus sur l'activation des licences, consultez Activation ou désactivation des licences facultatives, à la page 95.

Pour plus d'informations, voir le *Guide de commande Cisco AnyConnect*, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf. D'autres fiches techniques sont également disponibles sur http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/datasheet-listing.html.

Consignes et limites pour le VPN d'accès à distance

Veuillez tenir compte des consignes et limitations suivantes lors de la configuration du VPN d'accès à distance.

- Vous ne pouvez pas configurer à la fois l'accès (accès HTTPS dans la liste d'accès de gestion) FDM et le VPN SSL d'accès à distance sur la même interface, pour le même port TCP. Par exemple, si vous configurez le VPN SSL d'accès distant sur l'interface externe, vous ne pouvez pas ouvrir aussi l'interface externe pour les connexions HTTPS sur le port 443. Si vous configurez les deux fonctionnalités sur la même interface, veillez à modifier le port HTTPS d'au moins l'un de ces services pour éviter un conflit.
- L'interface externe du VPN d'accès à distance est un paramètre global. Vous ne pouvez pas configurer des profils de connexion distincts sur différentes interfaces.
- Vous ne pouvez pas utiliser des adresses qui se chevauchent dans l'adresse source d'une règle NAT et d'un ensemble d'adresses VPN d'accès à distance.
- Si vous configurez l'authentification à deux facteurs à l'aide des tokens RADIUS et RSA, le délai d'expiration d'authentification par défaut de 12 secondes est trop court pour permettre une authentification réussie dans la plupart des cas. Vous pouvez augmenter la valeur du délai d'expiration d'authentification en créant un profil client AnyConnect personnalisé et en l'appliquant au profil de connexion VPN d'accès à distance (RA VPN), comme décrit dans Configurer et charger les profils client AnyConnect, à la page 713. Nous recommandons un délai d'authentification d'au moins 60 secondes, afin que les utilisateurs aient suffisamment de temps pour s'authentifier, puis coller le token RSA, et pour la vérification aller-retour du token.

- L'émission de commandes telles que **curl** sur la tête de réseau du VPN d'accès à distance n'est pas directement prise en charge et pourrait ne pas donner les résultats souhaitables. Par exemple, la tête de réseau ne répond pas aux requêtes HTTP HEAD.
- Pour le VPN d'accès à distance, vous ne pouvez pas utiliser plusieurs objets de serveur SAML avec la même URL d'identifiant d'entité de fournisseur d'identité (IDP), même si les autres attributs sont différents. L'ID d'entité doit être unique pour tous les objets de serveur SAML utilisés dans les profils de connexion VPN d'accès à distance.

Configuration du VPN d'accès à distance

Pour activer le VPN d'accès à distance pour vos clients, vous devez configurer un certain nombre d'éléments distincts. La procédure suivante explique le processus de bout en bout.

Procédure

Étape 1 Configurer les licenses.

Vous devez activer deux licences :

- Lorsque vous enregistrez le périphérique, vous devez le faire avec un compte Smart Software Manager qui est activé pour les fonctionnalités d'exportation contrôlée. La licence de base doit respecter les exigences de contrôle des exportations avant de pouvoir configurer le VPN d'accès à distance. Vous ne pouvez pas non plus configurer la fonctionnalité à l'aide de la licence d'évaluation. Pour la procédure d'enregistrement du périphérique, consultez Enregistrement de l'appareil, à la page 93.
- Une licence VPN d'accès à distance. Pour de plus amples renseignements, consultez la section Exigences de licence pour le VPN d'accès à distance, à la page 710. Pour activer la licence, consultez Activation ou désactivation des licences facultatives, à la page 95.

Étape 2 Configurer les certificats.

Les certificats sont requis pour authentifier les connexions SSL entre les clients et le périphérique. Vous pouvez utiliser le DefaultInternalCertificate (Certificat interne par défaut) prédéfini pour le VPN, ou créer le vôtre.

Si vous utilisez une connexion chiffrée pour le domaine de répertoire utilisé pour l'authentification, vous devez charger un certificat d'autorité de certification de confiance.

Pour en savoir plus sur les certificats et la façon de les charger, consultez Configurer les certificats, à la page 160.

Étape 3 (Facultatif) Configurer les paramètres TLS/SSL.

Par défaut, le système permettra aux utilisateurs distants de se connecter au VPN d'accès à distance en utilisant toute version TLS et tout chiffrement pris en charge par le système. Cependant, vous pouvez limiter les versions TLS/DTLS, les chiffrements et les groupes Diffie-Hellman autorisés pour appliquer une connexion plus sécurisée. Consultez Configuration des paramètres de chiffrement TLS/SSL, à la page 815.

Étape 4 (Facultatif) Configurer et charger les profils client AnyConnect, à la page 713.

Étape 5 Configurer la source d'identité utilisée pour l'authentification des utilisateurs distants.

Vous pouvez utiliser les sources suivantes pour les comptes utilisateurs autorisés à se connecter au VPN d'accès à distance. Vous pouvez également utiliser des certificats clients pour l'authentification, seuls ou associés à une source d'identité.

- Active Directory identity realm (Domaine d'identité Active Directory) : en tant que source d'authentification principale. Les comptes d'utilisateur sont définis dans votre serveur Active Directory (AD). Consultez Configuration des domaines d'identité AD, à la page 171.
- RADIUS server group (Groupe de serveurs RADIUS) : en tant que source d'authentification principale ou secondaire, ainsi que pour l'autorisation et la comptabilité. Consultez Configurer les groupes de serveurs RADIUS, à la page 178.
- LocalIdentitySource (Base de données locale des utilisateurs) : en tant que source principale ou de repli. Vous pouvez définir des utilisateurs directement sur le périphérique et ne pas utiliser de serveur externe. Si vous utilisez la base de données locale comme source de secours, veillez à définir les mêmes noms d'utilisateur/mots de passe locaux que ceux définis dans le serveur externe. Consultez Configurer les utilisateurs locaux, à la page 187.
- Duo LDAP server (Serveur LDAP Duo) : en tant que source d'authentification principale ou secondaire. Bien que vous puissiez utiliser un serveur LDAP Duo comme source principale, il ne s'agit pas de la configuration normale. Vous l'utilisez normalement comme source secondaire pour fournir une authentification à deux facteurs en conjonction avec un serveur Active Directory ou RADIUS principal. Pour de plus amples renseignements, consultez la section Comment configurer l'authentification à deux facteurs à l'aide de Duo LDAP, à la page 745.
- **SAML** : utilise un serveur SAML comme source d'authentification principale. Lorsque vous utilisez SAML, vous ne pouvez pas configurer une source d'authentification de repli ou une source d'authentification secondaire. Pour de plus amples renseignements, consultez la section Configurer les serveurs SAML, à la page 184.

Étape 6 (Facultatif) Configurer les politiques de groupe pour le VPN d'accès à distance, à la page 726

La politique de groupe définit les attributs liés à l'utilisateur. Vous pouvez configurer des politiques de groupe pour fournir un accès différentiel aux ressources en fonction de l'appartenance au groupe. Vous pouvez également utiliser la politique par défaut pour toutes les connexions.

Étape 7 Configurer un profil de connexion VPN d'accès à distance, à la page 718.

Étape 8 Autoriser le trafic par le VPN d'accès à distance, à la page 715.

Étape 9 Vérifier la configuration VPN d'accès à distance, à la page 716.

Si vous rencontrez des problèmes pour effectuer une connexion, consultez Dépannage des VPN d'accès à distance, à la page 733.

Étape 10 (Facultatif) Activez la politique d'identité et configurez une règle pour l'authentification passive.

Si vous activez l'authentification passive des utilisateurs, les utilisateurs qui se sont connectés par le biais du VPN d'accès à distance seront affichés dans les tableaux de bord et ils seront également disponibles en tant que critères de correspondance de trafic dans les politiques. Si vous n'activez pas l'authentification passive, les utilisateurs de VPN d'accès à distance ne seront disponibles que s'ils correspondent à une politique d'authentification active. Vous devez activer la politique d'identité pour obtenir des informations de nom d'utilisateur dans les tableaux de bord ou pour la correspondance du trafic.

Configurer et charger les profils client AnyConnect

Les profilsclient AnyConnect sont téléchargés sur les clients avec le logiciel client AnyConnect. Ces profils définissent de nombreuses options liées au client, telles que la connexion automatique au démarrage et la reconnexion automatique, et si l'utilisateur final peut modifier l'option à partir des client AnyConnect préférences et des paramètres avancés.

Si vous configurez un nom d'hôte complet (FQDN) pour l'interface externe lors de la configuration de la connexion VPN d'accès à distance, le système crée un profil client pour vous. Ce profil active les paramètres par défaut. Vous ne devez créer et téléverser des profils client que si vous souhaitez un comportement autre que celui par défaut. Notez que les profils clients sont facultatifs : si vous n'en chargez pas, client AnyConnect utilisera les paramètres par défaut pour toutes les options contrôlées par profil.



Remarque Vous devez inclure l'interface externe du périphérique Firewall Threat Defense dans la liste des serveurs du profil VPN pour que le client AnyConnect affiche tous les paramètres contrôlables par l'utilisateur lors de la première connexion. Si vous n'ajoutez pas l'adresse ou le nom de domaine complet (FQDN) en tant qu'entrée d'hôte dans le profil, les filtres ne s'appliquent pas à la session. Par exemple, si vous créez une correspondance de certificat et que le certificat correspond correctement aux critères, mais que vous n'ajoutez pas le périphérique en tant qu'entrée d'hôte dans ce profil, la correspondance de certificat est ignorée.

Vous pouvez créer des profils pour le client AnyConnect ainsi que pour une variété de modules que vous pouvez éventuellement utiliser avec client AnyConnect, comme l'activateur AMP. Bien que vous puissiez charger des profils pour n'importe lequel de ces modules, le Gestionnaire de périphériques de pare-feu prend en charge la création du profil client AnyConnect uniquement. Cependant, vous pouvez charger n'importe quel type de profil par l'intermédiaire de Gestionnaire de périphériques de pare-feu, puis utiliser l'API Firewall Threat Defense (à partir d'API Explorer) pour modifier le type de profil de l'objet. La page des profils affiche tous les profils de tout type, bien que la liste n'indique pas le type de profil. La procédure explique comment procéder.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de profil client AnyConnect tout en modifiant une propriété de profil en cliquant sur le lien **Create New AnyConnect Client Profile (Créer un nouveau profil client AnyConnect)** affiché dans la liste des objets.

Avant de commencer

Avant de pouvoir téléverser des profils client, vous devez effectuer les opérations suivantes.

- Téléchargez et installez l'installateur autonome « Profile Editor - Windows / Standalone installer (MSI) ».client AnyConnect Le fichier d'installation est destiné à Windows uniquement et il est intitulé anyconnect-profileeditor-win-<version>-k9.msi, où <version> correspond à la version d'AnyConnect (le nom de fichier peut être modifié).client AnyConnect Par exemple, anyconnect-profileeditor-win-4.3.04027-k9.msi. Vous devez également installer Java JRE 1.6 (ou une version ultérieure) avant d'installer l'éditeur de profils. Obtenez l'éditeur de profil client AnyConnect auprès de software.cisco.com. Notez que ce paquet contient tous les éditeurs de profils, pas seulement celui du client VPN.
- Utilisez l'éditeur de profils pour créer les profils dont vous avez besoin. Vous devez préciser le nom d'hôte ou l'adresse IP de l'interface externe dans le profil. Pour des informations détaillées, consultez l'aide en ligne de l'éditeur.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **AnyConnect Client Profiles (Profils client AnyConnect)** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.
- Pour télécharger le profil associé à un objet, cliquez sur l'icône de téléchargement ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Saisissez un nom et, facultativement, une description pour l'objet.

Si vous chargez un profil de module, utilisez le nom de l'objet pour indiquer le type de module afin de vous permettre de le différencier plus facilement des profils client AnyConnect.

Étape 4 Cliquez sur **Upload** (Charger) et sélectionnez le fichier que vous avez créé à l'aide de l'éditeur de profil.

Étape 5 Cliquez sur **Open** (ouvrir) pour téléverser le profil.

Étape 6 Cliquez sur **OK** pour ajouter l'objet.

Étape 7 Si le profil que vous avez créé est en fait d'un type différent du profil client AnyConnect, procédez comme suit pour modifier le type de profil de l'objet.

a) Cliquez sur le bouton des autres options ( ) et choisissez **API Explorer** (Explorateur d'interface de protocole d'application).

Le système ouvre l'explorateur d'interface de protocole d'application dans un onglet ou une fenêtre distincte, en fonction des paramètres de votre navigateur.

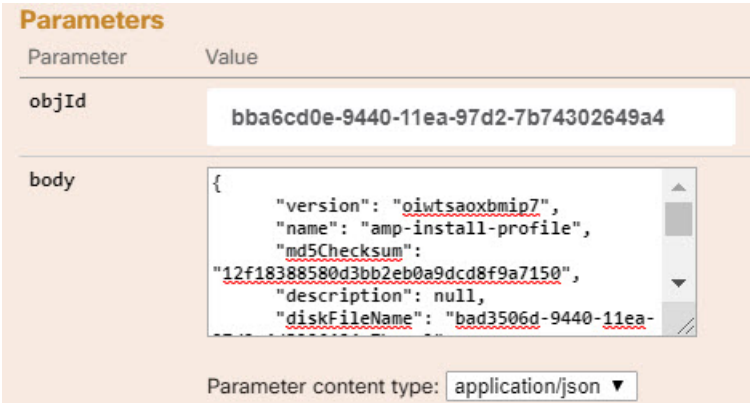
b) Ouvrez la ressource AnyConnectClientProfile.

c) Sélectionnez la méthodeGET /object/anyconnectclientprofiles et cliquez sur le bouton **Try It Out!** (Essayez-le !).

Chaque objet de profil sera représenté comme suit. L'attribut en surbrillance est celui que vous devez modifier.

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile",
      "links": {
        "self": "https://10.89.5.38/api/fdm/v6/object/
anyconnectclientprofiles/bba6cd0e-9440-11ea-97d2-7b74302649a4"
      }
```

d) Recherchez votre objet dans la sortie, sélectionnez le code et utilisez la touche Ctrl + cliquez pour le copier dans le presse-papier.
e) Sélectionnez la méthode PUT /object/anyconnectclientprofiles/{objId}, puis collez le contenu dans le champ **body** (corps).
f) Copiez la valeur **id** et collez-la dans la zone d'édition **objId** au-dessus du body (corps). Vous pouvez également trouver l'ID d'objet à la fin de l'URL « self ».



g) Dans le body (corps) de l'objet, recherchez le champ **anyConnectModuleType**, puis remplacez sa valeur par celle correspondant à votre type de profil. Choisissez parmi DART, FEEDBACK, WEB_SECURITY, ANY_CONNECT_CLIENT_PROFILE, AMP_ENABLER, NETWORK_ACCESS_MANAGER, NETWORK_VISIBILITY, START_BEFORE_LOGIN, ISE_POSTURE, UMBRELLA.
h) Toujours dans le **body** (corps), supprimez l'attribut **links**, y compris la virgule après la valeur **type**.

Le corps de l'objet doit ressembler à ce qui suit :

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "AMP_ENABLER",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile"
      }
```

i) Cliquez sur **Try It Out!** (Essayez-le!) Examinez la réponse afin de vérifier que l'objet a été correctement modifié. Vous devriez obtenir un code réponse de 200 et un corps de réponse qui reflète vos modifications. Vous pouvez utiliser la méthode GET pour vérifier davantage les résultats.

Autoriser le trafic par le VPN d'accès à distance

Vous pouvez utiliser l'une des techniques suivantes pour activer la circulation du trafic dans le tunnel VPN d'accès à distance.

- Configurez la commande **sysopt connection permit-vpn**, qui exempte le trafic qui correspond à la connexion VPN de la politique de contrôle d'accès. La valeur par défaut pour cette commande est **no sysopt connection permit-vpn**, ce qui signifie que le trafic VPN doit également être autorisé par la politique de contrôle d'accès.

Il s'agit de la méthode la plus sécurisée pour autoriser le trafic dans le VPN, car les utilisateurs externes ne peuvent pas falsifier des adresses IP dans l'ensemble d'adresses VPN d'accès à distance. L'inconvénient est que le trafic VPN ne sera pas inspecté, ce qui signifie que la protection contre les intrusions et les fichiers, le filtrage des URL ou d'autres fonctions avancées ne seront pas appliqués au trafic. Cela signifie également qu'aucun événement de connexion ne sera généré pour le trafic, et donc les tableaux de bord statistiques ne refléteront pas les connexions VPN.

Pour configurer cette commande, sélectionnez l'option **de politique de contournement du contrôle d'accès pour le trafic déchiffré dans vos profils de connexion VPN d'accès à distance**.

- Créez des règles de contrôle d'accès pour autoriser les connexions à partir de l'ensemble d'adresses VPN d'accès à distance. Cette méthode garantit que le trafic VPN est inspecté et que des services avancés peuvent être appliqués aux connexions. L'inconvénient est que des utilisateurs externes ont alors la possibilité de falsifier les adresses IP et d'accéder ainsi à votre réseau interne.

Vérifier la configuration VPN d'accès à distance

Après avoir configuré le VPN d'accès à distance et déployé la configuration sur le périphérique, vérifiez que vous pouvez établir des connexions à distance.

Si vous rencontrez des problèmes, lisez les rubriques de dépannage pour aider à isoler et à corriger les problèmes. Consultez Dépannage des VPN d'accès à distance, à la page 733.

Procédure

Étape 1 À partir d'un réseau externe, établissez une connexion VPN à l'aide du protocole client AnyConnect.

À l'aide d'un navigateur Web, ouvrez **https://***ravpn-address*, où *ravpn-address* est l'adresse IP ou le nom d'hôte de l'interface externe sur laquelle vous autorisez les connexions VPN. Si nécessaire, installez le logiciel client et terminez la connexion. Consultez Comment les utilisateurs peuvent installer le logiciel client AnyConnect, à la page 705.

Si vous avez modifié le port pour les connexions VPN d'accès à distance, vous devez inclure le port personnalisé dans l'URL. Par exemple, si vous avez changé le port en 4443 : https://ravpn.example.com:4443

Si vous avez configuré des URL de groupe, essayez également ces URL.

Étape 2 Connectez-vous à l'interface de ligne de commande du périphérique comme expliqué dans Connexion avec l'interface de ligne de commande (CLI), à la page 18. Sinon, ouvrez la console CLI.

Étape 3 Utilisez la commande **show vpn-sessiondb** pour afficher les informations récapitulatives sur les sessions VPN actuelles.

Les statistiques doivent afficher votre session client AnyConnect active et des informations sur les sessions cumulatives, le nombre maximal de sessions simultanées et les sessions inactives. Voici un exemple de sortie de la commande :

```
> show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
```

```
  SSL/TLS/DTLS               :      1 :         49 :           3 :        0
Clientless VPN               :      0 :          1 :           1
  Browser                    :      0 :          1 :           1
-----------------------------------------------------------------------------
Total Active and Inactive    :      1             Total Cumulative :     50
Device Total VPN Capacity    :  10000
Device Load                  :     0%
-----------------------------------------------------------------------------

-----------------------------------------------------------------------------
Tunnels Summary
-----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
Clientless                   :      0 :          1 :               1
AnyConnect-Parent            :      1 :         49 :               3
SSL-Tunnel                   :      1 :         46 :               3
DTLS-Tunnel                  :      1 :         46 :               3
-----------------------------------------------------------------------------
Totals                       :      3 :        142
-----------------------------------------------------------------------------

-----------------------------------------------------------------------------
IPv6 Usage Summary
-----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
AnyConnect SSL/TLS/DTLS      :        :           :
  Tunneled IPv6              :      1 :         20 :           2
-----------------------------------------------------------------------------
```

Étape 4 Utilisez la commande **show vpn-sessiondb anyconnect** pour afficher des informations détaillées sur les sessions VPN actuelles.

Les informations détaillées comprennent le chiffrement utilisé, les octets transmis et reçus et d'autres statistiques. Si vous utilisez votre connexion VPN, vous devriez voir les nombres d'octets transmis/reçus changer à mesure que vous réexécutez cette commande.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : priya                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone  : 0
```

Gestion de la configuration VPN d'accès à distance

Les profils de connexion VPN d'accès à distance définissent les caractéristiques qui permettent aux utilisateurs externes d'établir une connexion VPN avec le système à l'aide de client AnyConnect. Chaque profil définit les serveurs et les certificats AAA utilisés pour authentifier les utilisateurs, l'ensemble d'adresses pour attribuer des adresses IP aux utilisateurs et les politiques de groupe qui définissent une variété d'attributs axés sur l'utilisateur.

Vous créerez plusieurs profils si vous devez fournir des services variables à différents groupes d'utilisateurs ou si vous avez différentes sources d'authentification. Par exemple, si votre organisation fusionne avec une autre organisation qui utilise des serveurs d'authentification différents, vous pouvez créer un profil pour le nouveau groupe qui utilise ces serveurs d'authentification.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)**.

Le groupe affiche des informations récapitulatives sur le nombre de profils de connexion et de politiques de groupe actuellement configurés.

Étape 2 Cliquez sur **Connection Profiles** (Profils de connexion) dans la table des matières si ce n'est déjà fait.

Étape 3 Effectuez l'une des actions suivantes :

- Cliquez sur le bouton + pour créer un nouveau profil de connexion. Pour plus de renseignements sur les instructions, consultez Configurer un profil de connexion VPN d'accès à distance, à la page 718.
- Cliquez sur le bouton d'affichage ( ) pour ouvrir un résumé du profil de connexion et des instructions de connexion. Dans le résumé, vous pouvez cliquer sur **Edit** (Modifier) pour apporter des modifications.
- Cliquez sur le bouton de suppression ( ) pour supprimer un profil de connexion dont vous n'avez plus besoin.
- Sélectionnez **Group Policies** (Politiques de groupe) dans la table des matières afin de définir les attributs axés sur l'utilisateur pour les profils de connexion. Consultez Configurer les politiques de groupe pour le VPN d'accès à distance, à la page 726.

Configurer un profil de connexion VPN d'accès à distance

Vous pouvez créer un profil de connexion VPN d'accès à distance pour permettre à vos utilisateurs de se connecter à vos réseaux internes lorsqu'ils se trouvent sur des réseaux externes, comme leur réseau local. Créez des profils distincts pour tenir compte des différentes méthodes d'authentification.

Avant de commencer

Avant de configurer la connexion VPN d'accès à distance (RA)

- Téléchargez les paquets de logiciels client AnyConnect requis à partir de software.cisco.com sur votre ordinateur.
- L'interface externe, celle qui met fin aux connexions VPN d'accès à distance, ne peut pas également avoir une liste d'accès de gestion qui autorise les connexions HTTPS sur le même port. Configurez un port différent pour l'accès de gestion (voir Configuration du port HTTPS pour l'accès de gestion sur les interfaces de données, à la page 788) ou configurez un port différent pour le profil de connexion. Les deux services utilisent le port 443 par défaut, il faut donc le modifier.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)**.

Le groupe affiche des informations récapitulatives sur le nombre de profils de connexion et de politiques de groupe actuellement configurés.

Étape 2 Cliquez sur **Connection Profiles** (Profils de connexion) dans la table des matières si ce n'est déjà fait.

Étape 3 Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton + pour créer un nouveau profil de connexion.
- Cliquez sur le bouton d'affichage ( ) pour ouvrir un résumé du profil de connexion et des instructions de connexion. Dans le résumé, vous pouvez cliquer sur **Edit** (Modifier) pour apporter des modifications.

Étape 4 Configurez les attributs de connexion de base.

- **Connection Profile Name** (Nom du profil de connexion) : le nom de cette connexion, jusqu'à 50 caractères sans espaces. Par exemple, MainOffice. Vous ne pouvez pas utiliser une adresse IP comme nom.

  Remarque
  Le nom que vous saisissez ici est ce que les utilisateurs verront dans la liste des connexions du client AnyConnect. Choisissez un nom qui aura du sens pour vos utilisateurs.

- **Alias de groupe**, **URL de groupe** : les alias contiennent d'autres noms ou URL pour un profil de connexion spécifique. Les utilisateurs de VPN peuvent choisir un nom d'alias dans le client AnyConnect, dans la liste des connexions, lorsqu'ils se connectent au périphérique Firepower Threat Defense. Le nom de profil de connexion est automatiquement ajouté en tant qu'alias de groupe. Les alias peuvent comporter jusqu'à 31 caractères.

  Vous pouvez également configurer la liste des URL de groupe, que vos points terminaux peuvent sélectionner lors du lancement de la connexion VPN d'accès à distance. Si les utilisateurs se connectent à l'aide de l'URL de groupe, le système les connecte automatiquement en utilisant le profil de connexion qui correspond à cette dernière. Cette URL serait utilisée par les clients sur lesquels le client AnyConnect n'est pas encore installé.

  Ajoutez autant d'alias de groupe et d'URL que nécessaire. Ces alias et ces URL doivent être uniques pour tous les profils de connexion définis sur le périphérique. Les URL de groupe doivent commencer par **https://**.

  Par exemple, vous pouvez avoir l'alias Sous-traitant et l'URL de groupe https://ravpn.example.com/contractor. Une fois le client AnyConnect installé, l'utilisateur doit simplement sélectionner l'alias de groupe dans la liste déroulante de connexions VPN client AnyConnect.

Étape 5 Configurez les sources d'identité principales et, le cas échéant, secondaires.

Ces options déterminent la façon dont les utilisateurs distants s'authentifient sur le périphérique pour activer la connexion VPN d'accès à distance. L'approche la plus simple consiste à utiliser AAA uniquement, puis à sélectionner un domaine AD ou à utiliser LocalIdentitySource (LocalIdentitySource). Vous pouvez utiliser les approches suivantes pour **Authentication Type** (Type d'authentification) :

- **AAA Only** (AAA uniquement) : authentifie et autorise les utilisateurs en fonction du nom d'utilisateur et du mot de passe. Pour de plus amples renseignements, consultez la section Configurer AAA pour un profil de connexion, à la page 722.
- **Client Certificate Only** (Certificat client uniquement) : authentifie les utilisateurs en fonction du certificat d'identité du périphérique client. Pour de plus amples renseignements, consultez la section Configurer l'authentification par certificat pour un profil de connexion, à la page 725.
- **AAA et ClientCertificate** : utilise à la fois le nom d'utilisateur et le mot de passe ainsi que le certificat d'identité du périphérique client.
- **SAML** : utilise un serveur SAML comme source d'authentification principale. Lorsque vous utilisez SAML, vous ne pouvez pas configurer une source d'authentification de repli ou une source d'authentification secondaire. Pour de plus amples renseignements, consultez la section Configurer AAA pour un profil de connexion, à la page 722.

Étape 6 Configurez l'ensemble d'adresses pour les clients.

L'ensemble d'adresses définit les adresses IP que le système peut attribuer aux clients distants lorsqu'ils établissent une connexion VPN. Pour en savoir plus, consultez Configurer l'adressage client pour le VPN d'accès à distance, à la page 726.

Étape 7 Cliquez sur **Next** (suivant).

Étape 8 Sélectionnez la **Group Policy** (Politique de groupe) à utiliser pour ce profil.

La politique de groupe définit les conditions de connexion des utilisateurs après l'établissement du tunnel. Le système comprend une politique de groupe par défaut nommée « DfltGrpPolicy ». Vous pouvez créer des politiques de groupe supplémentaires pour fournir les services dont vous avez besoin.

Lorsque vous sélectionnez une politique de groupe, un résumé des caractéristiques du groupe s'affiche. Cliquez sur **Edit** (Modifier) dans le résumé pour apporter des modifications.

Si la politique de groupe dont vous avez besoin n'existe pas encore, cliquez sur **Create New Group Policy** (Créer une nouvelle politique de groupe) dans la liste déroulante.

Pour des informations détaillées sur les politiques de groupe, consultez Configurer les politiques de groupe pour le VPN d'accès à distance, à la page 726.

Étape 9 Cliquez sur **Next** (suivant).

Étape 10 Configurez les paramètres globaux.

Ces options s'appliquent à tous les profils de connexion. Après avoir créé le premier profil de connexion, ces options sont préconfigurées pour chaque profil suivant. Si vous apportez des modifications, vous modifiez tous les profils de connexion configurés.

- **Certificate of Device Identity** (Certificat d'identité du périphérique) : sélectionnez le certificat interne utilisé pour établir l'identité du périphérique. Les clients doivent accepter ce certificat pour établir une connexion VPN sécurisée. Si vous n'avez pas encore de certificat, cliquez sur **Create New Internal Certificate** (Créer un nouveau certificat interne) dans la liste déroulante. Vous devez configurer un certificat.

- **Outside Interface** (Interface externe) : l'interface à laquelle les utilisateurs se connectent lors de l'établissement de la connexion VPN d'accès à distance. Bien qu'il s'agisse normalement de l'interface externe (orientée Internet), choisissez l'interface située entre le périphérique et les utilisateurs finaux que vous prenez en charge.
- **Fully-qualified Domain Name for the Outside Interface** (Nom de domaine complet pour l'interface externe) : le nom de l'interface, par exemple, ravpn.exemple.com. Si vous spécifiez un nom, le système peut créer un profil client pour vous.

  Remarque
  Vous êtes responsable de vous assurer que les serveurs DNS utilisés dans le VPN et par les clients peuvent résoudre ce nom en l'adresse IP de l'interface externe. Ajoutez le nom de domaine complet aux serveurs DNS concernés.

- **Port** : le port TCP à utiliser pour les connexions VPN d'accès à distance. La valeur par défaut est 443. Si vous devez vous connecter à Gestionnaire de périphériques de pare-feu sur la même interface utilisée pour le VPN d'accès à distance, vous devez modifier le numéro de port soit pour le profil de connexion, soit pour Gestionnaire de périphériques de pare-feu. Les deux services utilisent le port 443 par défaut. Notez que les utilisateurs devront inclure le numéro de port dans l'URL si vous modifiez le port pour les connexions VPN d'accès à distance.
- **Bypass Access Control policy for decrypted traffic** (Contourner la politique de contrôle d'accès pour le trafic déchiffré) (sysopt permit-vpn) : indique si le trafic VPN est soumis à la politique de contrôle d'accès. Le trafic VPN déchiffré est soumis par défaut à l'inspection de la stratégie de contrôle d'accès. L'activation de l'option **Bypass Access Control policy for decrypted traffic** (Contourner la politique de contrôle d'accès pour le trafic déchiffré) contourne la politique de contrôle d'accès, mais pour le VPN d'accès à distance, le filtre ACL VPN et l'ACL d'autorisation téléchargée à partir du serveur AAA sont toujours appliqués au trafic VPN.

  Notez que si vous sélectionnez cette option, le système configure la commande **sysopt connection permit-vpn**, qui est un paramètre global. Cela aura également une incidence sur le comportement des connexions VPN de site à site. De plus, vous ne pouvez pas effectuer de sélections différentes pour cette option dans vos profils de connexion : la fonctionnalité est activée ou désactivée pour tous les profils.

  Si vous ne sélectionnez pas cette option, il pourrait être possible pour les utilisateurs externes d'usurper les adresses IP dans votre ensemble d'adresses VPN d'accès à distance et ainsi obtenir l'accès à votre réseau. Cela peut se produire parce que vous devrez créer des règles de contrôle d'accès qui permettent à votre ensemble d'adresses d'accéder aux ressources internes. Si vous utilisez des règles de contrôle d'accès, considérez l'utilisation des spécifications de l'utilisateur pour contrôler l'accès, plutôt que l'adresse IP source seule.

  L'inconvénient de sélectionner cette option est que le trafic VPN ne sera pas inspecté, ce qui signifie que la protection contre les intrusions et les fichiers, le filtrage des URL ou d'autres fonctions avancées ne seront pas appliqués au trafic. Cela signifie également qu'aucun événement de connexion ne sera généré pour le trafic, et donc les tableaux de bord statistiques ne refléteront pas les connexions VPN.
- **NAT Exempt** (Exemption NAT) : activez l'exemption NAT pour exempter de la traduction NAT le trafic vers et depuis les terminaux VPN d'accès à distance. Si vous n'exemptez pas le trafic VPN de la NAT, assurez-vous que les règles NAT existantes pour les interfaces externe et interne ne s'appliquent pas au bassin d'adresses du VPN d'accès à distance. Les règles d'exemption de NAT sont des règles NAT d'identité statique manuelle pour une combinaison interface source/destination et réseau donnée, mais elles ne sont pas reflétées dans la politique NAT, elles sont masquées. Si vous activez NAT exempté, vous devez également configurer les éléments suivants.

Notez qu'il s'agit d'une option globale; elle s'applique à tous les profils de connexion. Ainsi, ajoutez simplement des interfaces et des réseaux internes, ne les remplacez pas, sinon vous modifierez les paramètres d'exemption NAT pour tous les autres profils de connexion que vous avez déjà définis.

- **Inside Interfaces** (Interfaces internes) : sélectionnez les interfaces des réseaux internes auxquels les utilisateurs distants accéderont. Les règles NAT sont créées pour ces interfaces.
- **Inside Networks** (Réseaux internes) : sélectionnez les objets réseau qui représentent les réseaux internes auxquels les utilisateurs distants accèdent. La liste des réseaux doit contenir les mêmes types d'adresses IP que les ensembles d'adresses que vous prenez en charge.

- **AnyConnect Packages** (Paquets Secure Client / AnyConnect) : les images logicielles d'installation complète client AnyConnect que vous prendrez en charge sur les connexions VPN d'accès à distance. Pour chaque paquet, le nom de fichier, y compris les extensions, ne peut pas dépasser 60 caractères. Vous pouvez charger des paquets distincts pour les points terminaux Windows, Mac et Linux. Cependant, vous ne pouvez pas configurer différents paquets pour différents profils de connexion. Si vous avez déjà configuré un paquet pour un autre profil, le paquet est présélectionné. La modification de ce dernier le modifiera pour tous les profils.

  Téléchargez les paquets à partir de software.cisco.com. Si le terminal n'est pas déjà doté du bon paquet, le système invite l'utilisateur à télécharger et à installer le paquet après l'authentification de l'utilisateur.

Étape 11 Cliquez sur **Next** (suivant).

Étape 12 Examinez le résumé.

Tout d'abord, vérifiez que le résumé est correct.

Ensuite, cliquez sur **Instructions** pour voir ce que doivent faire les utilisateurs finaux pour installer initialement le logiciel client AnyConnect et vérifier qu'ils peuvent établir une connexion VPN. Cliquez sur **Copy** (Copier) pour copier ces instructions dans le presse-papiers, puis les distribuer à vos utilisateurs.

Étape 13 Cliquez sur **Terminer**.

Prochaine étape

Assurez-vous que le trafic est autorisé dans le tunnel VPN, comme expliqué dans la section Autoriser le trafic par le VPN d'accès à distance, à la page 715.

Configurer AAA pour un profil de connexion

Les serveurs d'authentification, d'autorisation et de comptabilité (AAA) utilisent un nom d'utilisateur et un mot de passe pour déterminer si un utilisateur est autorisé à accéder au VPN d'accès à distance. Si vous utilisez des serveurs RADIUS, vous pouvez différencier les niveaux d'autorisation des utilisateurs authentifiés afin de fournir un accès différentiel aux ressources protégées. Vous pouvez également utiliser les services de comptabilité RADIUS pour suivre l'utilisation.

Lors de la configuration de AAA, vous devez configurer une source d'identité principale. Les sources secondaires et de repli sont facultatives. Utilisez une source secondaire si vous souhaitez mettre en œuvre la double authentification, par exemple, à l'aide de jetons RSA ou de DUO.

Options de source d'identité principale

- **Primary Identity Source for User Authentication** (Source d'identité principale pour l'authentification de l'utilisateur) : la source d'identité principale utilisée pour authentifier les utilisateurs distants. Les utilisateurs finaux doivent être définis dans cette source ou dans la source de repli facultative pour pouvoir établir une connexion VPN. Sélectionnez l'une des options suivantes :
  - Un domaine d'identité Active Directory (AD). Si le domaine dont vous avez besoin n'existe pas encore, cliquez sur **Create New Identity Realm** (créer un nouveau domaine d'identité).
  - Un groupe de serveurs RADIUS.
  - LocalIdentitySource (la base de données des utilisateurs locaux) : vous pouvez définir des utilisateurs directement sur le périphérique et ne pas utiliser de serveur externe.
  - Un serveur LDAP Duo. Cependant, il est préférable de l'utiliser comme source d'authentification secondaire pour fournir une authentification à deux facteurs, comme décrit dans Comment configurer l'authentification à deux facteurs à l'aide de Duo LDAP, à la page 745. Si vous l'utilisez comme source principale, vous n'obtiendrez pas d'informations sur l'identité de l'utilisateur, et vous ne verrez pas les informations sur les utilisateurs dans les tableaux de bord, et vous ne pourrez pas non plus écrire de règles de contrôle d'accès basées sur l'utilisateur.
  - Un serveur SAML. Si vous utilisez un serveur SAML, vous ne pouvez pas configurer une source d'authentification de repli ou secondaire. Vous pouvez utiliser RADIUS comme serveur d'autorisation, mais vous devez configurer le serveur RADIUS pour que l'authentification ne soit pas requise. Autrement dit, le serveur RADIUS fournira les informations d'autorisation après l'authentification de la connexion par SAML.
- **Fallback Local Identity Source** (Source d'identité locale de secours) : si la source principale est un serveur externe, vous pouvez sélectionner LocalIdentitySource comme solution de repli au cas où le serveur principal ne serait pas disponible. Si vous utilisez la base de données locale comme source de secours, veillez à définir les mêmes noms d'utilisateur et mots de passe locaux que ceux définis sur le serveur externe.

Advanced Options (Options avancées)

- **Strip options** (Options de suppression) : un domaine est un domaine administratif. L'activation des options suivantes permet à l'authentification d'être basée sur le nom d'utilisateur uniquement. Vous pouvez activer n'importe quelle combinaison de ces options. Cependant, vous devez cocher les deux cases si votre serveur ne peut pas analyser les délimiteurs.
  - **Strip Identity Source Server from Username (Supprimer le serveur de source d'identité du nom d'utilisateur)** : que ce soit pour supprimer le nom de la source d'identité du nom d'utilisateur avant de transmettre ce nom au serveur AAA. Par exemple, si vous sélectionnez cette option et que l'utilisateur entre domaine\nom d'utilisateur comme nom d'utilisateur, le domaine est supprimé du nom d'utilisateur et envoyé au serveur AAA pour authentification. Par défaut, cette fonction est désactivée.
  - **Strip Group from Username** (Supprimer le groupe du nom d'utilisateur) : permet de supprimer le nom du groupe du nom d'utilisateur avant de transmettre ce nom au serveur AAA. Cette option s'applique aux noms donnés au format nomdutilisateur@domaine ; l'option supprime le domaine et le signe @. Par défaut, cette fonction est désactivée.

Source d'identité secondaire

- **Secondary Identity Source for User Authorization** (Source d'identité secondaire pour l'autorisation de l'utilisateur) : la deuxième source d'identité facultative. Si l'utilisateur s'authentifie avec succès auprès de la source principale, il est invité à s'authentifier auprès de la source secondaire. Vous pouvez sélectionner un domaine AD, un groupe de serveurs RADIUS, un serveur LDAP Duo, ou la source d'identité locale.
- **Advanced options** (Options avancées) : cliquez sur le lien **Advanced** (Avancé) et configurez les options suivantes
  - **Fallback Local Identity Source for Secondary** (Source d'identité locale de secours pour la source secondaire) : si la source secondaire est un serveur externe, vous pouvez sélectionner LocalIdentitySource comme solution de secours au cas où le serveur secondaire ne serait pas disponible. Si vous utilisez la base de données locale comme source de secours, veillez à définir les mêmes noms d'utilisateur/mots de passe locaux que ceux définis dans le serveur externe secondaire.
  - **Use Primary Username for Secondary Login** (Utiliser le nom d'utilisateur principal pour la connexion secondaire) : par défaut, lors de l'utilisation d'une source d'identité secondaire, le système vous demande de saisir le nom d'utilisateur et le mot de passe pour la source secondaire. Si vous sélectionnez cette option, le système invite uniquement à saisir le mot de passe secondaire et utilise pour la source secondaire le même nom d'utilisateur que celui authentifié auprès de la source d'identité principale. Sélectionnez cette option si vous configurez les mêmes noms d'utilisateur dans les sources d'identité principale et secondaire.
  - **Username for Session Server** (Nom d'utilisateur pour le serveur de session) : une fois l'authentification réussie, le nom d'utilisateur s'affiche dans les événements et les tableaux de bord statistiques, est utilisé pour déterminer les correspondances pour les règles de déchiffrement SSL et de contrôle d'accès basées sur l'utilisateur ou le groupe, et sert à la comptabilité. Comme vous utilisez deux sources d'authentification, vous devez indiquer au système s'il doit utiliser le nom d'utilisateur principal ou secondaire comme identité de l'utilisateur. Par défaut, le nom principal est utilisé.
  - **Password Type** (Type de mot de passe) : indique comment obtenir le mot de passe pour le serveur secondaire. Ce champ s'applique uniquement si vous sélectionnez **AAA et Client Certificate (certificat client)** pour le type d'authentification et pour les options de certificat, vous sélectionnez à la fois **Prefill username from certificate on user login window** (Préremplir le nom d'utilisateur à partir du certificat dans la fenêtre de connexion) et **Hide username in login window** (Masquer le nom d'utilisateur dans la fenêtre de connexion). La valeur par défaut est **Prompt** (Invite), ce qui signifie que l'utilisateur est invité à saisir le mot de passe.

    Sélectionnez **Primary Identity Source Password** (Mot de passe de la source d'identité principale) pour utiliser automatiquement le mot de passe saisi lors de l'authentification de l'utilisateur sur le serveur principal.

    Sélectionnez **Common Password** (Mot de passe commun) pour utiliser le même mot de passe pour chaque utilisateur, puis saisissez ce mot de passe dans le champ **Common Password** (Mot de passe commun).

Options supplémentaires

- **Authorization Server** (Serveur d'autorisation) : le groupe de serveurs RADIUS qui a été configuré pour autoriser les utilisateurs du VPN d'accès à distance.

Une fois l'authentification terminée, l'autorisation contrôle les services et les commandes disponibles pour chaque utilisateur authentifié. L'autorisation consiste à rassembler un ensemble d'attributs qui décrivent ce que l'utilisateur est autorisé à faire, ses capacités réelles et ses restrictions. Si vous n'utilisez pas l'autorisation, l'authentification à elle seule fournit le même accès à tous les utilisateurs authentifiés. Pour en savoir plus sur la configuration de RADIUS pour l'autorisation, consultez Contrôle des autorisations et des attributs des utilisateurs à l'aide de RADIUS et des stratégies de groupe, à la page 705.

Notez que si le système obtient des attributs d'autorisation du serveur RADIUS qui chevauchent ceux définis dans la group policy (stratégie de groupe), les attributs RADIUS remplacent les attributs de la stratégie de groupe.

- **Accounting Server** (Serveur de comptabilité) : (facultatif). Le groupe de serveurs RADIUS à utiliser pour prendre en compte la session VPN d'accès à distance.

  La fonction de traçabilité est utilisée pour suivre les services auxquels les utilisateurs accèdent et la quantité de ressources réseau qu'ils consomment. Le périphérique Firepower Threat Defense signale l'activité de l'utilisateur au serveur RADIUS. Les renseignements de comptabilité comprennent les heures de début et de fin des sessions, les noms d'utilisateur, le nombre d'octets transitant par le périphérique pour chaque session, le service utilisé et la durée de chaque session. Ces données peuvent ensuite être analysées pour la gestion du réseau, la facturation client ou l'audit. Vous pouvez utiliser la comptabilité seule ou conjointement avec l'authentification et l'autorisation.

Configurer l'authentification par certificat pour un profil de connexion

Vous pouvez utiliser les certificats installés sur le périphérique client pour authentifier les connexions VPN d'accès à distance.

Lorsque vous utilisez des certificats clients, vous pouvez toujours configurer une source d'identité secondaire, une source de repli et des serveurs d'autorisation et de comptabilité. Il s'agit d'options AAA ; pour en savoir plus, consultez Configurer AAA pour un profil de connexion, à la page 722.

Voici les attributs spécifiques au certificat. Vous pouvez configurer ces attributs séparément pour les sources d'identité principale et secondaire. La configuration d'une source secondaire est facultative.

- **Username from Certificate** (Nom d'utilisateur à partir du certificat) : sélectionnez l'une des options suivantes :
  - **Map Specific Field** (Mapper un champ spécifique) : utilisez les éléments de certificat dans l'ordre du **Primary Field** (Champ principal) et **Secondary Field** (Champ secondaire). Les valeurs par défaut sont CN (Common Name) et OU (Organizational Unit). Sélectionnez les options qui fonctionnent pour votre organisation. Les champs sont combinés pour fournir le nom d'utilisateur, et il s'agit du nom utilisé dans les événements, les tableaux de bord et, à des fins de correspondance, dans les règles de déchiffrement SSL et de contrôle d'accès.
  - **Utiliser le DN entier (nom distinctif) comme nom d'utilisateur** : le système dérive automatiquement le nom d'utilisateur des champs DN.
- **Options avancées** : cliquez sur le lien **Advanced** (Avancé) et configurez les options suivantes
  - **Préremplir le nom d'utilisateur à partir du certificat lors de la connexion de l'utilisateur** : indique s'il faut remplir le champ du nom d'utilisateur avec le nom récupéré lorsque l'utilisateur est invité à s'authentifier.

- **Masquer le nom d'utilisateur dans la fenêtre de connexion** : si vous sélectionnez l'option **Prefill** (Préremplirt), vous pouvez masquer le nom d'utilisateur, ce qui signifie que l'utilisateur ne peut pas le modifier dans l'invite de mot de passe.

Configurer l'adressage client pour le VPN d'accès à distance

Le système doit pouvoir fournir une adresse IP aux points terminaux qui se connectent au VPN d'accès à distance. Ces adresses peuvent être fournies par le serveur AAA, un serveur DHCP, un ensemble d'adresses IP configuré dans la politique de groupe ou un ensemble d'adresses IP configuré dans le profil de connexion. Le système teste ces ressources dans cet ordre et s'arrête lorsqu'il obtient une adresse disponible, qu'il attribue ensuite au client. Ainsi, vous pouvez configurer plusieurs options pour créer un mode à sécurité intégrée en cas d'un nombre peu commun de connexions simultanées.

Utilisez une ou plusieurs des méthodes suivantes pour configurer l'ensemble d'adresses d'un profil de connexion.

- **Serveur AAA** : d'abord, configurez un objet réseau sur le périphérique Firewall Threat Defense qui spécifie un sous-réseau pour l'ensemble d'adresses. Ensuite, dans le serveur RADIUS, configurez l'attribut Address-Pools (217) pour l'utilisateur portant le nom de l'objet. Précisez également le serveur RADIUS pour l'authentification dans le profil de connexion.
- **DHCP** : d'abord, configurez un serveur DHCP avec une ou plusieurs plages d'adresses IPv4 pour le VPN d'accès à distance (vous ne pouvez pas configurer les regroupements IPv6 à l'aide de DHCP). Créez ensuite un objet réseau d'hôte avec l'adresse IP du serveur DHCP. Vous pouvez ensuite sélectionner cet objet dans l'attribut **Serveurs DHCP** du profil de connexion. Vous pouvez configurer jusqu'à 10 serveurs DHCP.

  Si le serveur DHCP dispose de plusieurs ensembles d'adresses, vous pouvez utiliser l'attribut **de portée DHCP** dans la politique de groupe que vous ajoutez au profil de connexion pour sélectionner l'ensemble à utiliser. Créez un objet réseau hôte avec l'adresse réseau de l'ensemble. Par exemple, si l'ensemble DHCP contient 192.168.15.0/24 et 192.168.16.0/24, la définition de la portée de DHCP à 192.168.16.0 garantira qu'une adresse du sous-réseau 192.168.16.0/24 sera sélectionnée.
- **Ensembles d'adresses IP locales** : d'abord, créez jusqu'à six objets réseau qui précisent les sous-réseaux. Vous pouvez configurer des ensembles distincts pour IPv4 et IPv6. Ensuite, sélectionnez ces objets dans les options **IPv4 Address Pool** et **IPv6 Address Pool**, soit dans la politique de groupe, soit dans le profil de connexion. Vous n'avez pas besoin de configurer IPv4 et IPv6, configurez simplement le schéma d'adresse que vous souhaitez prendre en charge.

  Vous n'avez pas non plus besoin de configurer l'ensemble dans la politique de groupe et le profil de connexion. La politique de groupe remplace les paramètres de profil de connexion. Par conséquent, si vous configurez les ensembles dans la politique de groupe, laissez les options vides dans le profil de connexion.

  Notez que les ensembles sont utilisés dans l'ordre dans lequel vous les listez.

Configurer les politiques de groupe pour le VPN d'accès à distance

Une politique de groupe est un ensemble de paires d'attributs/valeurs axées sur l'utilisateur pour les connexions VPN d'accès à distance. Le profil de connexion utilise une politique de groupe qui définit les conditions des connexions d'utilisateur après l'établissement du tunnel. Les politiques de groupe vous permettent d'appliquer des ensembles complets d'attributs à un utilisateur ou à un groupe d'utilisateurs, plutôt que d'avoir à spécifier chaque attribut individuellement pour chaque utilisateur.

Le système comprend une politique de groupe par défaut nommée « DfltGrpPolicy ». Vous pouvez créer des politiques de groupe supplémentaires pour fournir les services dont vous avez besoin.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)**.

Le groupe affiche des informations récapitulatives sur le nombre de profils de connexion et de politiques de groupe actuellement configurés.

Étape 2 Cliquez sur **Group Policies** (Politiques de groupe) dans la table des matières.

Étape 3 Effectuez l'une des actions suivantes :

- Cliquez sur le bouton + pour créer un nouveau groupe. Consultez les rubriques suivantes pour obtenir des explications sur les attributs des pages de la politique de groupe :
  - Attributs généraux, à la page 727
  - Attributs des paramètres de session, à la page 728
  - Attributs d'attribution d'adresse, à la page 729
  - Attributs de tunnellisation fractionnée, à la page 729
  - Attributs client AnyConnect , à la page 730
  - Attributs des filtres de trafic, à la page 732
  - Attributs de mandataire de navigateur Windows, à la page 732
- Cliquez sur le bouton de modification ( ) pour modifier une politique existante.
- Cliquez sur le bouton de suppression ( ) pour supprimer un groupe dont vous n'avez plus besoin. Le groupe ne peut pas être actuellement utilisé dans un profil de connexion.

Attributs généraux

Les attributs généraux d'une politique de groupe définissent le nom du groupe et certains autres paramètres de base. L'attribut Name (Nom) est le seul attribut obligatoire.

- **Name** (Nom) : le nom de la politique de groupe. Le nom peut comporter jusqu'à 64 caractères. Les espaces sont autorisés.
- **Description** : une description de la politique de groupe. La description peut comporter jusqu'à 1 024 caractères.
- **Serveur DNS** : sélectionnez le groupe de serveurs DNS qui définit les serveurs DNS que les clients doivent utiliser pour la résolution de noms de domaine lorsqu'ils sont connectés au VPN. Si le groupe dont vous avez besoin n'est pas encore défini, cliquez sur **Create DNS Group** (créer un groupe DNS) et créez-le maintenant.

- **Bannière** : texte de la bannière, ou message de bienvenue, à présenter aux utilisateurs lors de la connexion. La valeur par défaut est Sans bannière. La longueur peut aller jusqu'à 496 caractères. La client AnyConnect ne prend en charge que le HTML partiel. Pour vous assurer que la bannière s'affiche correctement pour les utilisateurs distants, utilisez la balise
 pour indiquer les sauts de ligne.
- **Default Domain**(domaine par défaut) : le nom de domaine par défaut pour les utilisateurs de VPN d'accès à distance. Par exemple, exemple.com. Ce domaine est ajouté aux noms d'hôte qui ne sont pas complets, par exemple, serverA au lieu de serverA.example.com.
- **AnyConnect Client Profiles (Profils de client AnyConnect)** : cliquez sur **+** et sélectionnez les client AnyConnect profils à utiliser pour ce groupe. Si vous configurez un nom de domaine complet pour l'interface extérieure (dans le profil de connexion), un profil par défaut sera créé pour vous. Sinon, vous pouvez charger votre propre profil client. Créez ces profils à l'aide de l'éditeur de profils client AnyConnect autonome, que vous pouvez télécharger et installer à partir de software.cisco.com. Si vous ne sélectionnez pas de profil client, le client AnyConnect utilise les valeurs par défaut pour toutes les options. Les éléments de cette liste sont des objets Profil client AnyConnect plutôt que les profils eux-mêmes. Vous pouvez créer (et charger) de nouveaux profils en cliquant sur **Create New AnyConnect Client Profile (Créer un nouveau profil client AnyConnect)** dans la liste déroulante.

  Vous pouvez sélectionner des client AnyConnect profils de module, tels que AMP Enabler, en plus du profil client AnyConnect. Vous pouvez sélectionner un profil par type de module.

Attributs des paramètres de session

Les paramètres de session d'une politique de groupe contrôlent la durée de connexion des utilisateurs au VPN et le nombre de connexions distinctes qu'ils peuvent établir.

- **Maximum Connection Time** (Durée maximale de connexion) : la durée maximale, en minutes, pendant laquelle les utilisateurs peuvent rester connectés au VPN sans se déconnecter et se reconnecter, de 1 à 4 473 924, ou laisser le champ vide. La valeur par défaut est illimitée (vide), mais le délai d'inactivité s'applique toujours.
- **Connection Time Alert Interval** (Intervalle d'alerte de connexion) : si vous spécifiez une durée de connexion maximale, l'intervalle d'alerte définit le temps avant que la durée maximale ne soit atteinte pour afficher un avertissement à l'utilisateur concernant la déconnexion automatique à venir. L'utilisateur peut choisir de mettre fin à la connexion et de se reconnecter pour redémarrer le minuteur. La valeur par défaut est de 1 minute . Vous pouvez spécifier une valeur comprise entre 1 et 30 minutes.
- **Idle Time** (Durée d'inactivité) : la durée, en minutes, pendant laquelle la connexion VPN peut être inactive avant d'être close automatiquement, de 1 à 35 791 394. S'il n'y a aucune activité de communication sur la connexion pendant ce nombre consécutif de minutes, le système arrête la connexion. La valeur par défaut est de 30 minutes.
- **Idle Time Alert Interval** (Intervalle d'alerte de temps d'inactivité) : la durée avant que le temps d'inactivité ne soit atteint pour afficher un avertissement à l'utilisateur concernant la déconnexion automatique à venir en raison d'une session inactive. Toute activité réinitialise la minuterie. La valeur par défaut est de 1 minute . Vous pouvez spécifier une valeur comprise entre 1 et 30 minutes.
- **Simultaneous Login Per User** (Connexions simultanées par utilisateur) : nombre maximal de connexions simultanées autorisées pour un utilisateur. La valeur par défaut est de 3. Vous pouvez spécifier de 1 à 2147483647 connexions. Autoriser de nombreuses connexions simultanées peut compromettre la sécurité et affecter les performances.

Attributs d'attribution d'adresse

Les attributs d'attribution d'adresse d'une politique de groupe définissent l'ensemble des adresses IP pour le groupe. L'ensemble défini ici remplace l'ensemble défini dans tout profil de connexion qui utilise ce groupe. Laissez ce paramètre vide si vous souhaitez utiliser l'ensemble défini dans le profil de connexion.

- **IPv4 Address Pool** (Ensemble d'adresses IPv4), **IPv6 Address Pool** (Ensemble d'adresses IPv6) : ces options définissent les ensembles d'adresses pour les points terminaux distants. Les clients reçoivent une adresse de ces ensembles en fonction de la version IP qu'ils utilisent pour établir la connexion VPN. Sélectionnez un objet réseau qui définit un sous-réseau pour chaque type d'adresse IP que vous souhaitez prendre en charge. Laissez la liste vide si vous ne souhaitez pas prendre en charge cette version IP. Par exemple, vous pouvez définir un ensemble d'adresses IPv4 comme 10.100.10.0/24. L'ensemble d'adresses ne peut pas se trouver sur le même sous-réseau que l'adresse IP pour l'interface externe.

  Vous pouvez spécifier une liste de six ensembles d'adresses maximum à utiliser pour l'attribution d'adresses locale. L'ordre dans lequel vous spécifiez les ensembles est important. Le système attribue les adresses de ces ensembles dans l'ordre dans lequel les ensembles apparaissent.

- **DHCP Scope** (portée DHCP) : si vous configurez des serveurs DHCP pour l'ensemble d'adresses dans le profil de connexion, la portée DHCP identifie les sous-réseaux à utiliser pour l'ensemble d'adresses de ce groupe. Le serveur DHCP doit également avoir des adresses dans le même sous-réseau identifié par la portée. La portée vous permet de sélectionner un sous-ensemble des ensembles d'adresses définis dans le serveur DHCP à utiliser pour ce groupe précis.

  Si vous ne définissez pas de portée réseau, le serveur DHCP attribue les adresses IP dans l'ordre des ensembles d'adresses configurés. Il parcourt les ensembles jusqu'à ce qu'il identifie une adresse non attribuée.

  Pour spécifier une portée, sélectionnez un objet réseau contenant une adresse routable sur le même sous-réseau que l'ensemble d'adresses souhaité, mais à l'extérieur de cet ensemble. Le serveur DHCP détermine à quel sous-réseau cette adresse IP appartient et attribue une adresse IP de cet ensemble d'adresses.

  Nous vous recommandons d'utiliser l'adresse IP d'une interface chaque fois que cela est possible à des fins de routage. Par exemple, si l'ensemble d'adresses est 10.100.10.2-10.100.10.254 et que l'adresse d'interface est 10.100.10.1/24, utilisez 10.100.10.1 comme portée DHCP. N'utilisez pas le numéro de réseau. Cliquez sur **Create New Network** (créer un nouveau réseau) si l'objet n'existe pas. Vous ne pouvez utiliser DHCP que pour l'adressage IPv4. Si l'adresse que vous choisissez n'est pas une adresse d'interface, vous devrez peut-être créer une voie de routage statique pour l'adresse de portée.

Attributs de tunnellisation fractionnée

Les attributs de tunnellisation fractionnée d'une politique de groupe définissent la façon dont le système doit gérer le trafic destiné au réseau interne par rapport au trafic acheminé de l'extérieur. La tunnellisation fractionnée dirige une partie du trafic réseau dans le tunnel VPN (chiffré) et le trafic réseau restant à l'extérieur du tunnel VPN (non chiffré ou en texte clair).

- **IPv4 Split Tunneling** (Tunnelisation fractionnée IPv4), **IPv6 Split Tunneling** (Tunnelisation fractionnée IPv6) : vous pouvez spécifier différentes options selon que le trafic utilise des adresses IPv4 ou IPv6, mais les options pour les deux sont identiques. Si vous souhaitez activer la tunnellisation fractionnée, spécifiez l'une des options qui vous obligent à sélectionner des objets réseau.
  - **Allow all traffic over tunnel** (autoriser tout le trafic via le tunnel) : ne pas diviser la tunnellisation. Une fois que l'utilisateur établit une connexion VPN d'accès à distance, tout le trafic de l'utilisateur

passe par le tunnel protégé. Il s'agit du paramètre par défaut. Elle est également considérée comme l'option la plus sécurisée.

- **Allow specified traffic over the tunnel** (Autoriser le trafic spécifié sur le tunnel) : sélectionnez les objets réseau qui définissent le réseau de destination et les adresses d'hôte. Tout trafic vers ces destinations passe par le tunnel protégé. Le client achemine le trafic vers toute autre destination vers les connexions à l'extérieur du tunnel (comme une connexion Wi-Fi locale ou un réseau).
- **Exclude networks specified below** (Exclure les réseaux spécifiés ci-dessous) : sélectionnez les objets réseau qui définissent le réseau de destination ou les adresses d'hôte. Le client achemine tout trafic vers ces destinations vers des connexions à l'extérieur du tunnel. Le trafic vers toute autre destination passe par le tunnel.

- **Split DNS** (DNS fractionné) : vous pouvez configurer le système pour envoyer certaines requêtes DNS par l'intermédiaire de la connexion sécurisée tout en permettant au client d'envoyer d'autres requêtes DNS aux serveurs DNS configurés sur le client. Vous pouvez configurer les comportements DNS suivants :
  - **Send DNS Request as per split tunnel policy** (envoi d'une requête DNS conformément à la politique du tunnel fractionné) : avec cette option, les demandes DNS sont traitées de la même manière que les options de séparation du tunnel sont définies. Si vous activez la tunnellisation fractionnée, les requêtes DNS sont envoyées en fonction des adresses de destination. Si vous n'activez pas la tunnellisation fractionnée, toutes les requêtes DNS passent par la connexion protégée.
  - **Always send DNS requests over tunnel** (toujours envoyer les requêtes DNS via le tunnel) : sélectionnez cette option si vous activez la tunnellisation fractionnée, mais que vous souhaitez que toutes les requêtes DNS soient envoyées par la connexion protégée aux serveurs DNS définis pour le groupe.
  - **Send only specified domains over tunnel** (envoyer uniquement les domaines spécifiés via le tunnel) : sélectionnez cette option si vous souhaitez que vos serveurs DNS protégés résolvent les adresses de certains domaines uniquement. Ensuite, spécifiez ces domaines en séparant les noms de domaines par des virgules. Par exemple, exemple.com, exemple1.com. Utilisez cette option si vous souhaitez que vos serveurs DNS internes résolvent les noms des domaines internes, tandis que les serveurs DNS externes gèrent tout le reste du trafic Internet.

Attributs client AnyConnect

Les attributs client AnyConnect d'une politique de groupe définissent certains paramètres SSL et de connexion utilisés par le client AnyConnect pour une connexion VPN d'accès à distance.

Paramètres SSL

- **Enable Datagram Transport Layer Security (DTLS)** (activer la sécurité de la couche de transport des datagrammes, ou DTLS) : s'il faut autoriser le client AnyConnect à utiliser deux tunnels simultanément, un tunnel SSL et un tunnel DTLS. L'utilisation de DTLS évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets. Si vous n'activez pas DTLS, les utilisateurs du client AnyConnect qui établissent des connexions SSL VPN se connectent uniquement à l'aide d'un tunnel SSL.
- **DTLS Compression** (compression DTLS) : s'il faut compresser les connexions DTLS (Datagram Transport Layer Security) pour ce groupe à l'aide de LZS. La compression DTLS est désactivée par défaut.

- **SSL Compression (Compression SSL)**: indique s'il faut activer la compression des données et, si oui, la méthode de compression de données à utiliser, **Deflate** ou **LZS**. La compression SSL est **désactivée** par défaut. La compression des données accélère les débits de transmission, mais augmente également les besoins en mémoire et l'utilisation du processeur pour chaque session utilisateur. Par conséquent, la compression SSL diminue le débit global du périphérique.
- **SSL Rekey Method (Méthode de renouvellement de clé SSL)**, **SSL Rekey Interval (Intervalle de renouvellement de clé SSL)** : permet au client de renouveler la clé de la connexion VPN en renégociant les clés de chiffrement et les vecteurs d'initialisation afin d'augmenter la sécurité de la connexion. Désactivez le renouvellement de clé en sélectionnant **Aucun**. Pour activer rekey, sélectionnez **New Tunnel** pour créer un nouveau tunnel à chaque fois. (L'option **Existing Tunnel** (Tunnel existant) entraîne la même action que **New Tunnel** (Nouveau tunnel).) Si vous activez le renouvellement de clé, définissez également l'intervalle de renouvellement, qui est de 4 minutes par défaut. Vous pouvez définir l'intervalle entre 4 et 10 080 minutes (1 semaine).

Paramètres de connexion

- **Ignore DF (Don't Fragment) Bit**(ignorer le bit Ne pas fragmenter DF : s'il faut ignorer le bit Ne pas fragmenter (DF) dans les paquets qui ont besoin de fragmentation. Sélectionnez cette option pour autoriser la fragmentation forcée des paquets dont le bit DF est activé, afin que ces paquets puissent passer par le tunnel.
- **Client Bypass Protocol** (protocole de contournement client) : vous permet de configurer la façon dont la passerelle sécurisée gère le trafic IPv4 (lorsqu'elle s'attend uniquement au trafic IPv6) ou la façon dont elle gère le trafic IPv6 (lorsqu'elle s'attend uniquement au trafic IPv4).

  Lorsque client AnyConnect établit une connexion VPN avec la tête de réseau, celle-ci lui attribue une adresse IPv4, IPv6 ou aux deux une adresse IPv4 et IPv6. Si la tête de réseau affecte uniquement une adresse IPv4 ou IPv6 à la connexion client AnyConnect, vous pouvez configurer le protocole de contournement du client pour abandonner le trafic réseau pour lequel la tête de réseau n'a pas attribué d'adresse IP (par défaut, désactivé, non coché), ou autoriser que ce trafic contourne la tête de réseau et soit envoyé par le client non chiffré ou « en clair » (activé, coché).

  Par exemple, supposons que la passerelle sécurisée attribue uniquement une adresse IPv4 à la connexion client AnyConnect et que le point terminal fonctionne à deux niveaux. Lorsque le point terminal tente d'atteindre une adresse IPv6, si le protocole de contournement des clients est désactivé, le trafic IPv6 est abandonné; cependant, si le protocole de contournement client est activé, le trafic IPv6 est envoyé par le client en clair.
- **MTU** : taille maximale d'unité de transmission (MTU) pour les connexions de VPN SSL établies par client AnyConnect. Par défaut, c'est de 1406 octets. La plage se situe entre 576 et 1 462 octets.
- **Messages Keepalive entre AnyConnect et la passerelle VPN** : s'il faut échanger des messages Keepalive entre les homologues pour démontrer qu'ils sont disponibles pour envoyer et recevoir des données dans le tunnel. Les messages Keepalive sont transmis à des intervalles définis. L'intervalle par défaut est de 20 secondes, et la plage valide est de 15 à 600 secondes.
- **Intervalle DPD côté passerelle**, **Intervalle DPD côté client** : activez la fonction DPD (Dead peer detection) pour vous assurer que la passerelle VPN ou le client VPN détecte rapidement lorsque l'homologue ne répond plus. Vous pouvez activer séparément la passerelle ou le client DPD. L'intervalle par défaut est de 30 secondes pour l'envoi de messages DPD. L'intervalle peut aller de 5 à 3 600 secondes.

Attributs des filtres de trafic

Les attributs de filtre de trafic d'une politique de groupe définissent les restrictions que vous souhaitez imposer aux utilisateurs affectés au groupe. Vous pouvez utiliser ces attributs au lieu de créer des règles de politique de contrôle d'accès pour restreindre les utilisateurs de VPN d'accès à distance à des ressources spécifiques, en fonction de l'adresse et du protocole d'hôte ou de sous-réseau, ou du VLAN.

Par défaut, les utilisateurs de VPN d'accès à distance ne sont pas empêchés par la politique de groupe d'accéder à toute destination sur votre réseau protégé.

- **Access List Filter** (Filtre de liste d'accès) : limitez l'accès à l'aide d'une liste de contrôle d'accès étendue (ACL). Sélectionnez l'objet Smart CLI Extended ACL (ACL étendue Smart CLI), ou cliquez sur **Create Extended Access List** (Créer une liste d'accès étendue) et créez-la maintenant.

  La liste de contrôle d'accès étendue vous permet de filtrer par adresse source, adresse de destination et protocole (comme IP ou TCP). Les ACL sont évaluées sur une base descendante, à la première correspondance, alors faites en sorte de placer les règles spécifiques avant les règles plus générales. Il y a une règle implicite « refuser tout » à la fin de la liste de contrôle d'accès. Par conséquent, si vous avez l'intention de refuser l'accès à quelques sous-réseaux tout en autorisant tous les autres accès, assurez-vous d'inclure une règle « autoriser tout » à la fin de la liste de contrôle d'accès. Le filtre VPN s'applique aux connexions initiales uniquement. Il ne s'applique pas aux connexions secondaires, comme une connexion de support SIP, qui sont ouvertes en raison de l'action de l'inspection d'application.

  Comme vous ne pouvez pas créer d'objets réseau lors de la modification d'un objet d'interface de ligne de commande intelligente d'ACL étendue, vous devez créer la liste de contrôle d'accès avant de modifier la politique de groupe. Sinon, vous devrez peut-être simplement créer l'objet, puis revenir ultérieurement pour créer les objets de réseau et toutes les entrées de contrôle d'accès dont vous avez besoin. Pour créer la liste de contrôle d'accès, allez à **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)** > **Smart CLI** > **Objects (Objets)**, créez un objet puis sélectionnez **Extended Access List** (Liste d'accès étendue) comme type d'objet. Pour obtenir un exemple, consultez Comment contrôler l'accès VPN RA par groupe, à la page 772.

- **Restrict VPN to VLAN** (Restreindre le VPN au VLAN) : aussi appelé « VLAN mapping (mappage VLAN) », cet attribut précise l'interface VLAN de sortie pour les sessions auxquelles s'applique cette politique de groupe. Le système transfère tout le trafic de ce groupe vers le VLAN sélectionné.

  Utilisez cet attribut pour affecter un VLAN à la politique de groupe pour simplifier le contrôle d'accès. L'affectation d'une valeur à cet attribut est une alternative à l'utilisation d'une liste de contrôle d'accès pour filtrer le trafic sur une session. Assurez-vous de spécifier un numéro de VLAN défini sur une sous-interface du périphérique. Les valeurs sont comprises entre 1 et 4 094.

Attributs de mandataire de navigateur Windows

Les attributs de mandataire du navigateur Windows d'une politique de groupe déterminent si et comment fonctionne un mandataire défini dans le navigateur de l'utilisateur.

Vous pouvez sélectionner l'une des valeurs suivantes pour le **mandataire du navigateur pendant la session VPN** :

- **No change in endpoint settings**(pas de modification des paramètres de point terminal) : permet à l'utilisateur de configurer (ou de ne pas configurer) un mandataire de navigateur pour HTTP et d'utiliser le mandataire s'il est configuré.

- **Disable browser proxy** (Désactiver le mandataire de navigateur) : n'utilisez pas le mandataire défini pour le navigateur, le cas échéant. Aucune connexion du navigateur ne passera par le serveur mandataire.

- **Auto detect settings**(Paramètres de détection automatique) : activez l'utilisation de la détection automatique du serveur mandataire dans le navigateur pour la machine cliente.
- **Use custom settings** (Utiliser les paramètres personnalisés) : définissez un serveur mandataire qui doit être utilisé par tous les périphériques clients pour le trafic HTTP. Configurez les paramètres suivants :
  - **Proxy Server IP or Hostname (Adresse IP ou nom d'hôte du serveur mandataire)**, **Port** : adresse IP, ou nom d'hôte, du serveur mandataire et port utilisé pour les connexions proxy. La combinaison de l'hôte et du port ne peut pas dépasser 100 caractères.
  - **Browser Exemption List** (Liste d'exemptions de proxy pour navigateur) : les connexions aux hôtes ou ports figurant dans cette liste ne passent pas par le serveur mandataire. Ajoutez toutes les valeurs d'hôte et port pour les destinations qui ne doivent pas utiliser le serveur mandataire. Par exemple, www.exemple.com port 80. Cliquez sur le lien **Add** (Ajouter) pour ajouter des éléments à la liste. Cliquez sur l'icône de la corbeille pour supprimer des éléments. La liste d'exceptions de serveurs mandataires complète, en combinant l'ensemble des adresses et des ports, ne peut pas dépasser 255 caractères.

Surveillance du VPN d'accès à distance

Pour surveiller et dépanner les connexions VPN d'accès à distance, ouvrez la console CLI ou connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes.

- **show vpn-sessiondb** affiche les renseignements sur les sessions VPN. Vous pouvez réinitialiser ces statistiques à l'aide de la commande **clear vpn-sessiondb**.
- La commande **show webvpn** *keyword* affiche des renseignements sur la configuration du VPN d'accès à distance, y compris les statistiques et les images AnyConnect installées. Saisissez **show webvpn ?** pour afficher les mots-clés disponibles.
- **show aaa-server** affiche les statistiques sur le serveur de répertoire utilisé avec le VPN d'accès à distance.

Dépannage des VPN d'accès à distance

Les problèmes de connexion VPN d'accès à distance peuvent provenir du client ou de la configuration du périphérique Firewall Threat Defense. Les rubriques suivantes couvrent les principaux problèmes de dépannage que vous pourriez rencontrer.

Dépannage des problèmes de connexion SSL

Si l'utilisateur ne peut pas établir la connexion SSL initiale, non-client AnyConnect, avec l'adresse IP externe afin de télécharger client AnyConnect, procédez comme suit :

1. Si vous avez configuré un port autre que celui par défaut pour le profil de connexion VPN d'accès à distance, vérifiez que l'utilisateur inclut le numéro de port dans l'URL. Par exemple : https://ravpn.example.com:4443
2. À partir du poste de travail client, vérifiez que vous pouvez effectuer un ping vers l'adresse IP Si vous ne le pouvez pas, déterminez pourquoi il n'y a pas de routage entre le poste de travail de l'utilisateur et l'adresse.

3. À partir du poste de travail client, vérifiez que vous pouvez effectuer un ping vers le nom de domaine complet (FQDN) de l'interface externe, celui défini dans le profil de connexion VPN d'accès à distance (RA). Si vous pouvez pinguer l'adresse IP, mais pas le nom de domaine complet (FQDN), vous devez mettre à jour les serveurs DNS utilisés par le client et le profil de connexion VPN d'accès à distance (RA) afin d'ajouter le mappage FQDN–adresse IP.
4. Vérifiez que l'utilisateur accepte le certificat présenté par l'interface externe. L'utilisateur doit l'accepter définitivement.
5. Examinez la configuration de la connexion VPN d'accès à distance et vérifiez que vous avez sélectionné la bonne interface externe. Une erreur courante est de sélectionner une interface interne, celle faisant face aux réseaux internes, plutôt que l'interface externe, qui fait face aux utilisateurs de VPN d'accès à distance.
6. Si le chiffrement SSL est correctement configuré, utilisez un analyseur de paquets externe pour vérifier si l'établissement de liaison TCP à trois voies a réussi.

Dépannage des problèmes de téléchargement et d'installation client AnyConnect

Si l'utilisateur peut établir une connexion SSL avec l'interface externe, mais ne peut pas télécharger et installer le progiciel client AnyConnect, tenez compte des éléments suivants :

- Assurez-vous d'avoir chargé un paquet client AnyConnect pour le système d'exploitation du client. Par exemple, si le poste de travail de l'utilisateur exécute Linux, mais que vous n'avez pas chargé d'image Linux client AnyConnect, aucun paquet ne pourra être installé.
- Pour les clients Windows, l'utilisateur doit disposer de droits d'administrateur pour installer le logiciel.
- Pour les clients Windows, le poste de travail doit activer ActiveX ou installer Java JRE 1.5 ou version ultérieure, avec JRE 7 recommandé.
- Pour les navigateurs Safari, Java doit être activé.
- Essayez différents navigateurs, l'un d'eux pourrait échouer alors qu'un autre réussit.

Dépannage des problèmes de connexionclient AnyConnect

Si l'utilisateur a pu se connecter à l'interface externe, télécharger et installer client AnyConnect, mais n'a pas pu ensuite établir une connexion à l'aide de client AnyConnect, tenez compte des éléments suivants :

- Si vous utilisez DHCP pour fournir des adresses IP au client et que le client ne peut pas obtenir d'adresse, vérifiez les règles NAT. Toute règle NAT qui s'applique au réseau VPN d'accès à distance doit inclure l'option de recherche de routage. La recherche de routage peut permettre de s'assurer que les requêtes DHCP sont envoyées au serveur DHCP par l'intermédiaire d'une interface appropriée.
- Si l'authentification échoue, vérifiez que l'utilisateur saisit le bon nom d'utilisateur et le bon mot de passe, et que le nom d'utilisateur est défini correctement dans le serveur d'authentification. Le serveur d'authentification doit également être disponible dans l'une des interfaces de données.

Remarque Si le serveur d'authentification se trouve sur un réseau externe, vous devez configurer une connexion VPN de site à site avec le réseau externe et inclure l'adresse de l'interface VPN d'accès à distance dans le VPN. Pour de plus amples renseignements, consultez la section Comment utiliser un serveur de répertoire sur un réseau externe avec le VPN d'accès à distance, à la page 757.

- Si vous avez configuré un nom de domaine complet (FQDN) pour l'interface externe dans le profil de connexion VPN d'accès à distance (RA), vérifiez que vous pouvez pinguer le FQDN à partir du périphérique client. Si vous pouvez pinguer l'adresse IP, mais pas le nom de domaine complet (FQDN), vous devez mettre à jour les serveurs DNS utilisés par le client et le profil de connexion VPN d'accès à distance (RA) afin d'ajouter le mappage FQDN–adresse IP. Si vous utilisez le profil par défaut client AnyConnect qui est généré lorsque vous spécifiez un nom de domaine complet pour l'interface externe, l'utilisateur devra modifier l'adresse du serveur pour utiliser l'adresse IP jusqu'à ce que le DNS soit mis à jour.
- Vérifiez que l'utilisateur accepte le certificat présenté par l'interface externe. L'utilisateur doit l'accepter définitivement.
- Si le client AnyConnect de l'utilisateur comprend plusieurs profils de connexion, qu'il sélectionne le bon.
- Si tout semble correct du côté du client, établissez une connexion SSH avec le périphérique Firewall Threat Defense et entrez la commande **debug webvpn** [ ]. Examinez les messages émis lors d'une tentative de connexion.

Dépannage des problèmes de flux de trafic du VPN d'accès à distance

Si l'utilisateur peut établir une connexion VPN d'accès à distance sécurisé (RA), mais ne peut pas envoyer et recevoir le trafic, procédez comme suit :

1. Demandez au client de se déconnecter, puis de se reconnecter. Parfois, cela élimine le problème.
2. Dans client AnyConnect, vérifiez les statistiques de trafic pour déterminer si les compteurs envoyés et reçus augmentent. Si le nombre de paquets reçus reste à zéro, le périphérique Firewall Threat Defense ne renvoie aucun trafic. Il y a probablement un problème dans la configuration Firewall Threat Defense. Les problèmes courants sont les suivants :
   - Les règles d'accès bloquent le trafic. Vérifiez la stratégie de contrôle d'accès pour connaître les règles qui empêchent le trafic entre les réseaux internes et l'ensemble des adresses du VPN d'accès à distance. Vous devrez peut-être créer une règle Allow (Autoriser) explicite si votre action par défaut est de bloquer le trafic.
   - Le filtre VPN bloque le trafic. Vérifiez le filtre de trafic d'ACL ou le filtre de VLAN configuré dans la politique de groupe pour le profil de connexion. Vous devrez peut-être effectuer des ajustements dans l'ACL ou modifier le VLAN, selon la façon (ou si) vous filtrez le trafic en fonction de la politique de groupe.
   - Les règles de NAT ne sont pas contournées pour le trafic VPN d'accès à distance. Assurez-vous que l'exemption de NAT est configurée pour la connexion VPN d'accès à distance pour chaque interface interne. Sinon, vérifiez que les règles de NAT n'affectent pas la communication entre les réseaux et les interfaces internes et l'ensemble d'adresses VPN d'accès à distance et l'interface externe.

- Les routes sont mal configurées. Assurez-vous que toutes les routes définies sont valides et fonctionnent correctement. Par exemple : si une adresse IP statique est définie pour l'interface externe, assurez-vous que la table de routage comprend une route par défaut (pour 0.0.0.0/0 et ::/0).
- Assurez-vous que le serveur DNS et le nom de domaine configurés pour le VPN d'accès à distance sont corrects et que le système client utilise les appropriés. Vérifiez que les serveurs DNS sont accessibles.
- Si vous activez la tunnellisation fractionnée dans le VPN d'accès à distance, vérifiez si le trafic vers les réseaux internes spécifiés passe par le tunnel, tandis que tout autre trafic contourne le tunnel (de sorte que le périphérique Firewall Threat Defense ne le voit pas).

3. Établissez une connexion SSH avec le périphérique Firewall Threat Defense et vérifiez que le trafic est envoyé et reçu pour le VPN d'accès à distance. Utilisez les commandes suivantes :
   - **show webvpn anyconnect**
   - **show vpn-sessiondb**

Exemples d'utilisation du VPN d'accès à distance

Voici des exemples de configuration d'un VPN d'accès à distance.

Comment mettre en œuvre la modification d'autorisation RADIUS

Le changement d'autorisation (CoA) RADIUS, aussi appelé autorisation dynamique, assure la sécurité des points terminaux pour le VPN d'accès à distance Firepower Threat Defense. Un défi clé pour les VPN d'accès à distance est de sécuriser le réseau interne contre les points terminaux compromis et de sécuriser le point terminal lui-même lorsqu'il est affecté par des virus ou des programmes malveillants, en corrigeant l'attaque sur le point terminal. Il est nécessaire de sécuriser le point terminal et le réseau interne à toutes les étapes, c'est-à-dire avant, pendant et après la session VPN d'accès à distance. La fonctionnalité RADIUS CoA aide à atteindre cet objectif.

Si vous utilisez des serveurs RADIUS Cisco Identity Services Engine (ISE), vous pouvez configurer l'application de la politique de modification d'autorisation.

La fonctionnalité de changement d'autorisation ISE fournit un mécanisme pour modifier les attributs d'une session d'authentification, d'autorisation et de comptabilité (AAA) après son établissement. Lorsqu'une politique est modifiée pour un utilisateur ou un groupe d'utilisateurs dans AAA, ISE envoie des messages CoA au périphérique Firepower Threat Defense pour réinitialiser l'authentification et appliquer la nouvelle politique. Un point d'application de posture en ligne (IPEP) n'est pas nécessaire pour appliquer les listes de contrôle d'accès (ACL) à chaque session VPN établie avec le périphérique Firepower Threat Defense.

Les attributs que vous pouvez modifier au cours de le CoA sont l'URL de redirection, l'ACL de redirection et la balise de groupe de sécurité.

Les rubriques suivantes expliquent comment fonctionne le CoA et comment le configurer.

Flux système pour la modification d'autorisation

Cisco ISE dispose d'un agent de posture client qui évalue la conformité d'un point terminal pour des critères tels que les processus, les fichiers, les entrées de registre, la protection antivirus, la protection contre les

logiciels espions et les logiciels de pare-feu installés sur l'hôte. Les administrateurs peuvent ensuite restreindre l'accès au réseau jusqu'à ce que le terminal soit conforme, ou rehausser les privilèges de l'utilisateur local afin qu'il puisse mettre en place des mesures correctives. ISE Posture effectue une évaluation côté client. Le client reçoit d'ISE la politique d'exigences de posture, effectue la collecte des données de posture, compare les résultats à la politique et renvoie les résultats de l'évaluation à ISE.

Voici le flux système entre le périphérique Firepower Threat Defense, ISE et le client VPN d'accès à distance (RA) pour le traitement de la modification d'autorisation (CoA).

1. L'utilisateur distant démarre une session VPN d'accès à distance à l'aide de client AnyConnect, avec le périphérique Firepower Threat Defense.
2. Le périphérique Firepower Threat Defense envoie un message de demande d'accès RADIUS pour cet utilisateur au serveur ISE.
3. Comme la posture du client est inconnue à ce stade, ISE fait correspondre l'utilisateur à la politique d'autorisation configurée pour une posture inconnue. Cette politique définit les options cisco-av-pair suivantes, qu'ISE envoie à Firepower Threat Defense dans une réponse RADIUS Access-Accept.
   - **url-redirect-acl=***acl_name*, où *acl_name* est le nom d'une liste de contrôle d'accès étendue configurée sur le périphérique Firepower Threat Defense. Cette liste de contrôle d'accès définit le trafic d'utilisateur qui doit être redirigé vers le serveur ISE, qui est le trafic HTTP. Par exemple :

     ```
     url-redirect-acl=redirect
     ```

   - **url-redirect=***url*, où l'URL est celle vers laquelle le trafic doit être redirigé. Par exemple :

     ```
     url-redirect=https://ise2.example.com:8443/guestportal/gateway?sessionId=xx&action=cpp
     ```

   Vous devez configurer le DNS pour les interfaces de données afin que le nom d'hôte puisse être résolu. Si vous configurez également le filtrage du trafic dans la politique de groupe pour le profil de connexion, vérifiez que l'ensemble de clients peut atteindre le serveur ISE par le port (TCP/8443 dans l'exemple).
4. Le périphérique Firepower Threat Defense envoie un paquet de début de demande de comptabilité RADIUS et reçoit une réponse d'ISE. La demande de comptabilité comprend tous les détails de la session, y compris l'ID de session, l'adresse IP externe du client VPN et l'adresse IP du périphérique Firepower Threat Defense. ISE utilise l'ID de session pour identifier cette session. Le périphérique Firepower Threat Defense envoie également des informations de comptabilité intérimaire périodiques, dont l'attribut le plus important est Framed-IP-Address, contenant l'adresse IP attribuée au client par le périphérique Firepower Threat Defense.
5. Lorsqu'il est dans un état de posture inconnu, le périphérique Firepower Threat Defense redirige le trafic du client qui correspond à l'ACL de redirection vers l'URL de redirection. ISE détermine si le client dispose du module de conformité de posture requis et invite l'utilisateur à l'installer au besoin.
6. Une fois l'agent installé sur le périphérique client, il effectue automatiquement les vérifications configurées dans la politique de posture ISE. Le client communique directement avec ISE. Il envoie un rapport de posture à ISE, lequel peut inclure plusieurs échanges utilisant le protocole SWISS et les ports TCP/UDP 8905.
7. Lorsqu'ISE reçoit le rapport de posture de l'agent, il traite à nouveau les règles d'autorisation. Cette fois, le résultat de la posture est connu et une règle différente correspond maintenant au client. ISE envoie un paquet RADIUS CoA, qui inclut une liste de contrôle d'accès téléchargeable (DACL) pour les points terminaux conformes ou non conformes. Par exemple, la DACL conforme peut autoriser tous les accès,

tandis que la DACL non conforme refuse tous les accès. Le contenu de la DACL relève de l'administrateur ISE.

8. Le périphérique Firepower Threat Defense supprime la redirection. S'il n'a pas les listes de contrôle d'accès en cache, il doit envoyer une demande d'accès afin de les télécharger à partir d'ISE. La DACL spécifique est associée à la session VPN ; elle ne fait pas partie de la configuration du périphérique.
9. La prochaine fois que l'utilisateur du VPN d'accès à distance tente d'accéder à la page Web, il peut accéder aux ressources autorisées par la DACL installée sur le périphérique Firepower Threat Defense pour la session.



Remarque Si le point terminal ne satisfait pas à une exigence obligatoire et qu'une correction manuelle est requise, une fenêtre de correction s'ouvre dans le client AnyConnect, affichant les éléments nécessitant une intervention. La fenêtre de correction s'exécute en arrière-plan afin que les mises à jour de l'activité du réseau ne s'affichent pas et n'interfèrent pas ou ne provoquent pas de perturbations. Un utilisateur peut cliquer sur **Details** (Détails) dans la partie vignette de la posture ISE du client AnyConnect afin de voir ce qui a été détecté et les mises à jour requises avant de pouvoir rejoindre le réseau.

Configurer Change of Authorization (modification d'autorisation) sur le périphérique Firewall Threat Defense

La majeure partie de la politique Change of Authorization (changement d'autorisation) est configurée dans le serveur ISE. Cependant, vous devez configurer le périphérique Firepower Threat Defense pour une connexion correcte à ISE. La procédure suivante explique comment configurer le côté Firepower Threat Defense de la configuration.

Avant de commencer

Si vous utilisez des noms d'hôte dans un objet, veillez à configurer les serveurs DNS à utiliser avec les interfaces de données, comme expliqué dans la section Configuration DNS pour les données et le trafic de gestion, à la page 798. Vous devez généralement configurer le DNS de toute façon pour avoir un système entièrement fonctionnel.

Procédure

Étape 1 Configurez la liste de contrôle d'accès (ACL) étendue pour rediriger les connexions initiales vers ISE.

L'objectif de la liste de contrôle d'accès de redirection est d'envoyer le trafic initial à ISE afin qu'ISE puisse évaluer la posture du client. La liste de contrôle d'accès doit envoyer le trafic HTTPS à ISE, mais pas le trafic déjà destiné à ISE ou le trafic dirigé vers un serveur DNS pour la résolution de nom. Un exemple d'ACL de redirection peut ressembler à ce qui suit :

```
access-list redirect extended deny ip any host <ISE server IP>
access-list redirect extended deny ip any host <DNS server IP>
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
```

Cependant, notez que les listes de contrôle d'accès ont un « deny any any » (refuser tout) implicite comme dernière entrée de contrôle d'accès (ACE). Dans cet exemple, la dernière ACE, qui correspond au port TCP

www (c'est-à-dire au port 80), ne correspondra à aucun trafic correspondant aux 3 premières ACE, qui sont donc redondantes. Vous pouvez simplement créer une liste de contrôle d'accès avec la dernière ACE et obtenir les mêmes résultats.

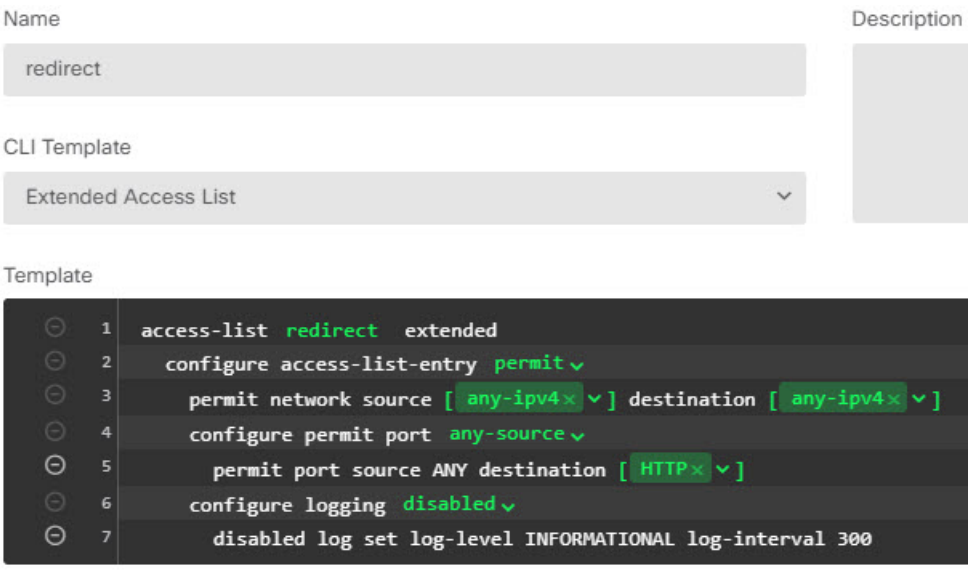
Notez que dans une liste de contrôle d'accès de redirection, les actions permit (autoriser) et deny (refuser) déterminent simplement quel trafic correspond à la liste de contrôle d'accès, avec permit correspondant et deny ne correspondant pas. Aucun trafic n'est réellement abandonné, le trafic refusé n'est tout simplement pas redirigé vers ISE.

Pour créer la liste de contrôle d'accès de redirection, vous devez configurer un objet Smart CLI.

a) Choisissez **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)** > **Smart CLI** > **Objects (Objets)**.
b) Cliquez + pour créer un nouvel objet.
c) Saisissez un nom pour la liste de contrôle d'accès. Par exemple, **rediriger**.
d) Pour **CLI Template** (Modèle CLI), sélectionnez **Extended Access List** (Liste d'accès étendue).
e) Configurez les éléments suivants dans le **corps du modèle** :

- configurer l'action de liste d'accès = autoriser
- réseau-source = any-ipv4
- réseau-destination = any-ipv4
- configurer autoriser port = any-source
- port-destination = HTTP
- configurer la journalisation = désactivée

L'ACE doit ressembler à ce qui suit :



f) Cliquez sur **OK**.

Cette liste de contrôle d'accès sera configurée lors du prochain déploiement de modifications. Vous n'avez pas besoin d'utiliser l'objet dans une autre politique pour forcer le déploiement.

Remarque

Cette liste de contrôle d'accès s'applique uniquement à IPv4. Si vous voulez également prendre en charge IPv6, ajoutez simplement une deuxième ACE avec tous les mêmes attributs, sauf que vous devez sélectionner any-ipv6 pour les réseaux source et de destination. Vous pouvez également ajouter les autres ACE pour vous assurer que le trafic vers le serveur ISE ou vers le serveur DNS n'est pas redirigé. Vous devrez d'abord créer des objets de réseau hôtes pour contenir les adresses IP de ces serveurs.

Étape 2 Configurer un groupe de serveurs RADIUS pour l'autorisation dynamique.

Il existe plusieurs options essentielles que vous devez sélectionner correctement dans le serveur RADIUS et les objets de groupe de serveurs pour activer la modification d'autorisation, également connue sous le nom d'autorisation dynamique. La procédure suivante se concentre sur ces attributs. Pour plus de détails sur ces objets, consultez Serveurs et groupes RADIUS, à la page 176.

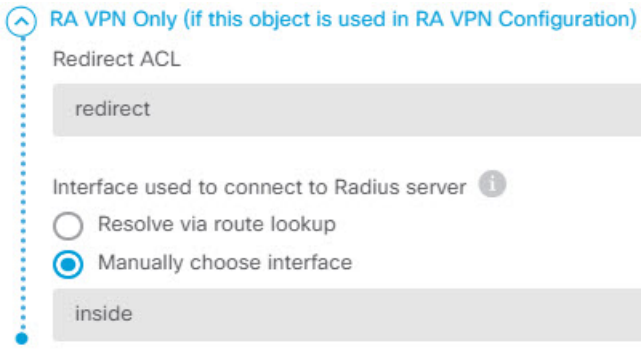
a) Choisissez **Objects (Objets)** > **Identity Sources (Sources d'identité)**.
b) Cliquez sur **+** > **RADIUS Server** (Serveur RADIUS).
c) Saisissez un nom pour le serveur, ainsi que le nom d'hôte/l'adresse IP du serveur ISE RADIUS, le port d'authentification et la clé secrète configurés sur le serveur. Ajustez le délai d'expiration si vous le souhaitez. Ces options ne sont pas directement liées à l'autorisation dynamique.
d) Cliquez sur le lien RA VPN Only (RA VPN uniquement) et configurez les options suivantes :

- **Redirect ACL**(ACL de redirection) —sélectionnez la liste de contrôle d'accès étendue que vous avez créée pour la redirection. Dans cet exemple, l'ACL nommée redirect.
- **Interface used to connect to Radius server** (Interface utilisée pour la connexion au serveur RADIUS) —sélectionnez **Manually Choose Interface** (Sélectionner l'interface manuellement, puis sélectionnez l'interface par laquelle le serveur peut être atteint. Vous devez sélectionner une interface spécifique pour que le système puisse activer correctement l'écouteur CoA sur celle-ci.

  Si le serveur se trouve sur le même réseau que l'adresse de gestion, ce qui signifie que vous sélectionnerez l'interface de diagnostic, vous devez également configurer une adresse IP sur l'interface de diagnostic. Il n'est pas suffisant d'avoir une adresse IP de gestion. Accédez à **Device (Périphérique)** > **Interfaces**, et configurez une adresse IP sur l'interface de diagnostic qui se trouve sur le même sous-réseau que l'adresse IP de gestion.

  Si vous utilisez également ce serveur pour l'accès administratif Gestionnaire de périphériques de pare-feu, cette interface est ignorée. Les tentatives d'accès administratif sont toujours authentifiées au moyen de l'adresse IP de gestion.

L'exemple suivant montre les options configurées pour l'interface interne.



e) Cliquez sur **OK** pour enregistrer l'objet serveur.

Si vous avez une configuration redondante avec plusieurs serveurs ISE RADIUS en double, créez des objets serveur pour chacun de ces serveurs.

f) Cliquez sur **+** > **RADIUS Server Group** (Groupe de serveurs RADIUS.
g) Saisissez un nom pour le groupe de serveurs et ajustez le temps mort et le nombre maximal de tentatives si vous le souhaitez.
h) Sélectionnez l'option **Dynamic Authorization** (Autorisation dynamique) et modifiez le numéro de port si votre serveur ISE est configuré pour utiliser un port différent. Le port 1700 est le port par défaut utilisé pour l'écoute des paquets CoA.
i) Si le serveur RADIUS est configuré pour utiliser un serveur AD pour authentifier les utilisateurs, sélectionnez le **domaine qui prend en charge le serveur RADIUS** qui spécifie le serveur AD utilisé en liaison avec ce serveur RADIUS. Si le domaine n'existe pas déjà, cliquez sur **Create New Identity Realm** (Créer un nouveau domaine d'identité au bas de la liste et configurez-le maintenant.
j) Sous **RADIUS Server** (Serveur RADIUS), cliquez sur **+** et sélectionnez l'objet serveur que vous avez créé pour le VPN d'accès à distance.
k) Cliquez sur **OK** pour enregistrer l'objet du groupe de serveurs.

Étape 3 Choisissez **Device (Périphérique)** > **RA VPN (VPN d'accès à distance)** > **Connection Profiles (Profils de connexion**, puis créez un profil de connexion qui utilise ce groupe de serveurs RADIUS.

Utilisez **l'authentification AAA** (uniquement ou avec des certificats) et sélectionnez le groupe de serveurs dans la **source d'identité principale pour les options d'authentification de l'utilisateur**, **d'autorisation** et **de comptabilité**.

Configurez toutes les autres options en fonction des besoins de votre organisation.

Remarque
Si les serveurs DNS sont accessibles via le réseau VPN, modifiez la politique de groupe utilisée dans le profil de connexion pour configurer l'option **Split DNS** (DNS fractionnée) sur la page Split Tunneling Attributes (Attributs de tunnellisation fractionnée).

Configurer la modification d'autorisation dans ISE

La majeure partie de la configuration de changement d'autorisation est effectuée dans le serveur ISE. ISE dispose d'un agent d'évaluation de posture qui fonctionne sur le périphérique terminal, et ISE communique directement avec le périphérique pour déterminer la position de posture. Le périphérique Firepower Threat Defense attend essentiellement les instructions d'ISE sur la façon de gérer un utilisateur final donné.

Une description complète de la configuration des politiques d'évaluation de la posture n'entre pas dans le cadre de ce document. Cependant, la procédure suivante explique certains des principes de base. Utilisez-le comme point de départ pour la configuration d'ISE. Notez que les chemins de commande exacts, les noms de page et les noms d'attribut peuvent changer d'une version à l'autre. La version d'ISE que vous utilisez peut utiliser une terminologie ou une organisation différente.

La version ISE minimale prise en charge est de 2.2 correctif 1.

Avant de commencer

Cette procédure suppose que vous ayez déjà configuré les utilisateurs dans le serveur ISE RADIUS.

Procédure

Étape 1 Choisissez **Administration** > **Network Resources (Ressources réseau)** > **Network Devices (Périphériques réseau)** > **Network Devices (Périphériques réseau)**, ajoutez le périphérique Firepower Threat Defense à l'inventaire des périphériques réseau ISE et configurez les paramètres RADIUS.

Sélectionnez les **RADIUS Authentication Settings** (Paramètres d'authentification RADIUS) et configurez le même **Shared Secret** (Secret partagé) que celui configuré dans l'objet serveur RADIUS Firepower Threat Defense. Si vous le souhaitez, modifiez le numéro **de port CoA** et veillez à configurer le même port dans l'objet de groupe de serveurs RADIUS Firepower Threat Defense.

Étape 2 Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Results (Résultats)** > **Authorization (Autorisation)** > **Downloadable ACLs (ACL téléchargeables)**.

Créez 2 listes de contrôle d'accès téléchargeables (DACL), une pour une utilisation par des points terminaux conformes, et une pour les points terminaux non conformes.

Par exemple, vous pouvez autoriser tous les accès pour les points terminaux conformes (autoriser ip any any), tout en refusant tout accès aux points terminaux non conformes (refuser ip any any). Vous pouvez rendre ces listes de contrôle d'accès aussi complexes que vous le souhaitez, pour fournir l'accès exact que les utilisateurs doivent avoir en fonction de leur état de conformité. Vous utiliserez ces listes de contrôle d'accès dans les profils d'autorisation.

Étape 3 Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Results (Résultats)** > **Authorization (Autorisation)** > **Authorization Profile (Profil d'autorisation)**, puis configurez les profils requis.

Vous avez besoin de profils pour les états suivants. Les attributs minimaux pour chacun sont répertoriés.

- **Unknown** (Inconnu) : le profil de posture inconnu est le profil de posture par défaut. Chaque terminal est mis en correspondance avec cette politique lors de l'établissement initial de la connexion VPN d'accès à distance. Le point de cette règle est d'appliquer la liste de contrôle d'accès et l'URL de redirection, et de télécharger l'agent de posture s'il n'est pas déjà sur le point terminal. Les points terminaux peuvent rester associés à ce profil si l'agent n'est pas installé ou si l'installation échoue. Sinon, après avoir évalué la posture, les points terminaux passent aux profils conforme ou non conforme.

  Les attributs minimaux incluent les suivants :

  - **Name** (Nom) : par exemple, PRE_POSTURE.
  - **Access Type** (Type d'accès) : sélectionnez **ACCESS_ACCEPT**.
  - **Common Tasks** (Tâches courantes) : sélectionnez **Web Redirection** (Redirection Web) (CWA, MDM, NSP, CPP), puis **Client Provisioning** (Provisionnement de client) (Posture), et saisissez le nom de l'ACL de redirection que vous avez configurée sur le périphérique Firepower Threat Defense. Dans **Value** (Valeur), sélectionnez **Client Provisioning Portal** (Portail de provisionnement client) s'il n'est pas déjà sélectionné.
  - Les **Attribute Details** (Détails de l'attribut) doivent afficher deux valeurs cisco-av-pair, pour url-redirect-acl et url-redirect. ISE enverra ces données au périphérique Firepower Threat Defense, qui appliquera les critères à la session utilisateur du VPN d'accès à distance.

- **Compliant (Conforme)**: après la fin de l'évaluation de la posture, si le point terminal respecte toutes les exigences configurées, le client est considéré comme conforme et reçoit ce profil. Vous donneriez généralement à ce client un accès complet.

  Les attributs minimaux incluent les suivants :

  - **Name** (Nom) : par exemple, FULL_ACCESS.
  - **Access Type** (Type d'accès) : sélectionnez **ACCESS_ACCEPT**.
  - **Common Tasks** (Tâches courantes) : sélectionnez **DACL Name**, puis la liste de contrôle d'accès téléchargeable pour les utilisateurs conformes, par exemple, PERMIT_ALL_TRAFFIC. ISE enverra la liste de contrôle d'accès au périphérique Firepower Threat Defense, qui l'appliquera à la session utilisateur. Cette liste de contrôle d'accès remplacera l'ACL de redirection initiale pour la session utilisateur.

- **Non-compliant** (Non conforme) : si l'évaluation de la posture détermine que le point terminal ne satisfait pas à toutes les exigences, un compte à rebours démarre pendant lequel le client peut mettre le terminal en conformité, par exemple en installant les mises à jour requises. Le client AnyConnect informe l'utilisateur des problèmes de conformité. Pendant le compte à rebours, le terminal reste dans l'état de conformité inconnu. Si le point terminal reste non conforme après l'expiration du compte à rebours, la session est marquée comme non conforme et elle obtient le profil non conforme. Vous devez généralement empêcher tout accès pour ce point terminal ou au moins restreindre l'accès d'une manière ou d'une autre.

  Les attributs minimaux incluent les suivants :

  - **Name** (Nom) : par exemple, Non_Compliant.
  - **Access Type** (Type d'accès) : sélectionnez **ACCESS_ACCEPT**.
  - **Common Tasks** (Tâches courantes) : sélectionnez **DACL Name**, puis la liste de contrôle d'accès téléchargeable pour les utilisateurs non conformes, par exemple, DENY_ALL_TRAFFIC. ISE enverra la liste de contrôle d'accès au périphérique Firepower Threat Defense, qui l'appliquera à la session utilisateur. Cette liste de contrôle d'accès remplacera l'ACL de redirection initiale pour la session utilisateur.

Étape 4 Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Results (Résultats)** > **Client Provisioning (Provisionnement de client)** > **Resources (Ressources)**, puis configurez les ressources suivantes :

- **AnyConnect package** (Package AnyConnect) : le fichier de package head-end, que vous téléchargez depuis software.cisco.com. Vous avez besoin de packages distincts pour les plateformes client prises en charge ; vous devrez donc peut-être configurer plusieurs types, comme AnyConnectDesktopWindows.
- **ISE Posture Configuration File** (Fichier de configuration de posture ISE) : ce fichier de configuration définit les paramètres utilisés par le module de conformité pour évaluer le périphérique de l'utilisateur final. Ce fichier définit également le délai dont dispose l'utilisateur pour mettre en conformité un périphérique non conforme.
- **Compliance Module Package** (Package du module de conformité) (Type : ComplianceModule) : le fichier du module de conformité client AnyConnect est distribué vers le package AnyConnect installé afin de vérifier la conformité du point terminal. Téléchargez ce fichier à l'aide de la commande **Add Resource from Cisco Site** (Ajouter une ressource à partir du site Cisco). Assurez-vous de téléchargerle module approprié en fonction des packages client AnyConnect configurés, sans quoi les utilisateurs

rencontreront des échecs de téléchargement. Vous pouvez également trouver ces fichiers sur software.cisco.com dans les listes client AnyConnect du dossier ISEComplianceModule.

- **AnyConnect Configuration File** (Fichier de configuration AnyConnect) (Type : AnyConnectConfig) : ces paramètres spécifiques à la version client AnyConnect définissent le **AnyConnect Package** (Package AnyConnect), le **Compliance Module (Module de conformité)** et la **ISE Posture (Posture ISE)** à appliquer. Comme les paquets sont propres au système d'exploitation, créez des fichiers de configuration distincts pour chaque SE client pris en charge (par exemple : Windows, Mac, Linux).

Étape 5 Choisissez **Policy (Politique)** > **Client Provisioning (Provisionnement de client)**, puis configurez la politique de provisionnement de client.

Créez de nouvelles règles, par exemple avec des noms comme CoA_ClientProvisionWin, pour chaque système d'exploitation devant mettre en œuvre CoA. Sélectionnez le système d'exploitation approprié pour la règle et, dans **Results** (Résultats), sélectionnez le fichier de configuration client AnyConnect créé pour ce système d'exploitation en tant qu'**Agent**.

Désactivez les règles par défaut propres au système d'exploitation que vous remplacez.

Étape 6 Configurez la politique de posture.

Au cours de cette étape, vous développez les exigences de posture qui ont du sens pour votre organisation.

- Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Conditions** > **Posture**, puis définissez les conditions de posture simples à respecter. Par exemple, vous pouvez exiger que l'utilisateur ait certaines applications installées.
- Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Results (Résultats)** > **Posture** > **Exigences**, puis définissez l'exigence du module de conformité pour le point terminal.
- Choisissez **Politiques** > **Posture** > **Politique de posture** et configurez les politiques pour les systèmes d'exploitation pris en charge.

Étape 7 Choisissez **Policy (Politique)** > **Policy Sets (Ensembles de politiques)** > **Default (Par défaut)** > **Authorization Policy (Politique d'autorisation)**, puis créez la politique.

Ajoutez des règles pour chacune des conditions de conformité. Ces exemples de valeurs sont basés sur les exemples des étapes précédentes.

- Inconnu, pour la pré-posture et le téléchargement de posture.
  - Name (Nom) : par exemple, PRE_POSTURE.
  - Conditions : « Session-PostureStatus EST ÉGAL À Inconnu » ET « Radius-NAS-Port-Type EST ÉGAL À Virtual »
  - Profiles (Profils) : par exemple, PRE_POSTURE
- Conforme, pour les clients qui répondent aux exigences de posture.
  - Name (Nom) : par exemple, FULL_ACCESS.
  - Conditions : « Session-PostureStatus EST ÉGAL À Conforme » ET « Radius-NAS-Port-Type EST ÉGAL À Virtual »
  - Profiles (Profils) : par exemple, FULL_ACCESS

- Non-conformité, pour les clients qui ne parviennent pas aux exigences de posture.
  - Name (Nom) : par exemple, NON-COMPLIANT
  - Conditions : « Session-PostureStatus EST ÉGAL À NonConforme » ET « Radius-NAS-Port-Type EST ÉGAL À Virtual »
  - Profiles (Profils) : par exemple, Non_Compliant

Étape 8 (Facultatif) Choisissez **Administration** > **Settings (Paramètres)** > **Posture** > **Reassessments (Réévaluations)**, puis activez la réévaluation de la posture.

Par défaut, la posture est évaluée au moment de la connexion uniquement. Vous pouvez activer la réévaluation de la posture pour vérifier périodiquement la posture des points terminaux connectés. Vous pouvez définir l'intervalle de réévaluation pour déterminer la fréquence à laquelle cela se produit.

Si le système échoue lors de la réévaluation, vous pouvez définir la réponse du système. Vous pouvez autoriser l'utilisateur à continuer (rester connecté), le déconnecter ou lui demander de corriger le système.

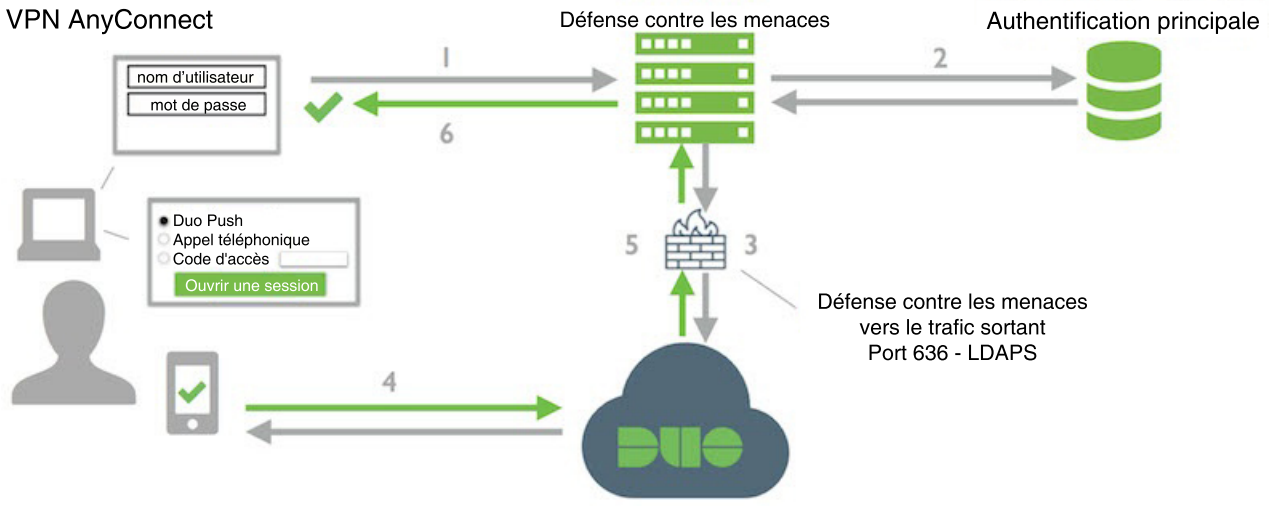
Comment configurer l'authentification à deux facteurs à l'aide de Duo LDAP

Vous pouvez utiliser le serveur LDAP Duo comme source d'authentification secondaire en conjonction avec un serveur Microsoft Active Directory (AD) ou RADIUS comme source principale. Avec Duo LDAP, l'authentification secondaire valide l'authentification principale avec un code d'accès Duo, une notification poussée ou un appel téléphonique.

Les rubriques suivantes expliquent la configuration plus en détail.

Flux système pour l'authentification secondaire Duo LDAP

Le graphique suivant montre comment le Firepower Threat Defense et Duo fonctionnent ensemble pour fournir une authentification à deux facteurs à l'aide de LDAP.



Voici une explication du flux système :

1. L'utilisateur établit une connexion VPN d'accès à distance avec le périphérique Firepower Threat Defense et fournit un nom d'utilisateur et un mot de passe.
2. Firewall Threat Defense authentifie cette tentative d'authentification principale auprès du serveur d'authentification principal, qui peut être Active Directory ou RADIUS.
3. Si l'authentification principale réussit, le Firepower Threat Defense envoie une demande d'authentification secondaire au serveur Duo LDAP.
4. Duo authentifie ensuite l'utilisateur séparément, par notification poussée, message texte avec code d'accès ou appel téléphonique. L'utilisateur doit terminer cette authentification avec succès.
5. Duo répond au périphérique Firepower Threat Defense pour indiquer si l'utilisateur s'est authentifié avec succès.
6. Si l'authentification secondaire a réussi, le périphérique Firepower Threat Defense établit une connexion VPN d'accès à distance avec le client AnyConnect de l'utilisateur.

Configurer l'authentification secondaire Duo LDAP

La procédure suivante explique le processus de bout en bout de configuration de l'authentification à deux facteurs, en utilisant Duo LDAP comme source d'authentification secondaire, pour le VPN d'accès à distance. Notez que vous devez avoir un compte auprès de Duo et obtenir certaines informations auprès de Duo pour terminer cette configuration.

Procédure

Étape 1 Créez un compte Duo et obtenez la clé d'intégration, la clé secrète et le nom d'hôte API.

Voici un aperçu du processus. Pour en savoir plus, consultez le site Web de Duo, https://duo.com.

a) Inscrivez-vous pour un compte Duo.
b) Connectez-vous au Duo Admin Panel (panneau d'administration Duo) et accédez à **Applications**.
c) Cliquez sur **Protect an Application** (Protéger une application) et recherchez le VPN SSL de Cisco dans la liste des applications. Cliquez sur **Protect this Application** (Protéger cette application) pour obtenir votre clé d'intégration, votre clé secrète et votre nom d'hôte API. Pour obtenir de l'aide, consultez le *guide de démarrage* Duo, https://duo.com/docs/getting-started.

Étape 2 Créez une source d'identité LDAP Duo pour le serveur LDAP Duo.

Vous devez utiliser l'API Firepower Threat Defense pour créer l'objet LDAP Duo; vous ne pouvez pas le créer à l'aide de Gestionnaire de périphériques de pare-feu. Vous pouvez soit utiliser API Explorer (Explorateur API), soit écrire votre propre application cliente pour créer l'objet. La procédure suivante explique comment créer l'objet à l'aide de API Explorer (Explorateur API).

a) Dans le Gestionnaire de périphériques de pare-feu, cliquez sur le bouton des autres options (⋮) et choisissez **API Explorer** (Explorateur API.

Le système ouvre l'explorateur d'interface de protocole d'application dans un onglet ou une fenêtre distincte, en fonction des paramètres de votre navigateur.

b) (Facultatif) Obtenez les valeurs nécessaires pour identifier l'interface que le système doit utiliser pour se connecter au serveur LDAP Duo.

Si vous ne précisez pas d'interface, le système utilise la table de routage. Si nécessaire, vous pouvez créer une route statique pour le serveur Duo LDAP. Sinon, vous pouvez préciser l'interface à utiliser dans l'objet LDAP Duo. Si vous souhaitez préciser l'interface, utilisez les différentes méthodes GET dans le groupe Interfaces pour obtenir les valeurs nécessaires. Vous pouvez utiliser des interfaces physiques, de sous-interface, EtherChannel ou VLAN. Par exemple, pour obtenir les valeurs d'une interface physique, utilisez la méthode GET /devices/default/interfaces et recherchez l'objet correspondant à l'interface que vous devez utiliser. Vous avez besoin des valeurs suivantes de l'objet d'interface :

- ID
- type
- version
- name

c) Cliquez sur l'en-tête **DuoLDAPIdentitySource** pour ouvrir le groupe.
d) Cliquez sur la méthode **POST /object/duoldapidentitysources**.
e) Sous l'en-tête **Parameters** (Paramètres), pour l'élément **body** (corps, cliquez dans la zone d'affichage **Example Value** (Valeur d'exemple) dans la colonne **Data Type** (Type de données) à droite. Cette action charge l'exemple dans la zone d'édition de la valeur du corps.
f) Dans la zone d'édition de la **valeur du corps**, procédez comme suit :

- Supprimez les lignes d'attributs suivantes : **version**, **id**. (Ces attributs sont nécessaires pour les appels PUT, mais pas pour POST.)
- Pour **name**, saisissez un nom pour l'objet, tel que Duo-LDAP-server.
- Pour **description**, saisissez une description significative de l'objet à des fins de référence ou supprimez la ligne d'attribut.
- Pour **apiHostname**, saisissez le nom d'hôte API que vous avez obtenu de votre compte Duo. Le nom d'hôte doit ressembler à ce qui suit, en remplaçant toutefois les X par votre valeur unique : API-XXXXXXXX.DUOSECURITY.COM. Les majuscules ne sont pas obligatoires.
- Pour **port**, saisissez le port TCP à utiliser pour LDAPS. Il doit s'agir du port 636, à moins que Duo ne vous ait demandé d'utiliser un autre port. Notez que vous devez vous assurer que votre liste de contrôle d'accès autorise le trafic vers le serveur Duo LDAP par l'intermédiaire de ce port.
- Pour **timeout**, saisissez le délai d'expiration, en secondes, pour la connexion au serveur Duo. La valeur peut être comprise entre 1 et 300 secondes. La valeur par défaut est de 120 secondes. Pour utiliser la valeur par défaut, saisissez 120 ou supprimez la ligne d'attribut.
- Pour **integrationKey**, saisissez la clé d'intégration que vous avez obtenue de votre compte Duo.
- Pour **secretKey**, saisissez la clé secrète que vous avez obtenue de votre compte Duo. Cette clé sera ensuite masquée.
- Pour **interface**, saisissez les valeurs id, type, version et name de l'interface à utiliser pour la connexion au serveur Duo LDAP ou supprimez les 6 lignes utilisées pour définir l'attribut d'interface, y compris l'accolade de fermeture.
- Pour **type**, laissez la valeur duoldapidentitysource.

Par exemple, le corps de l'objet peut ressembler à ce qui suit, où apiHostname et integrationKey sont masqués, mais la clé secrète falsifiée intentionnellement est affichée :

```
{
  "name": "Duo-LDAP-server",
  "description": "Duo LDAP server for RA VPN",
  "apiHostname": "API-XXXXXXXX.DUOSECURITY.COM",
  "port": 636,
  "timeout": 120,
  "integrationKey": "XXXXXXXXXXXXXXXXXXXX",
  "secretKey": "123456789",
  "type": "duoldapidentitysource"
}
```

g) Cliquez sur le bouton **Try It Out!** (Essayez-le !).

Le système émettra la commande **curl** pour publier l'objet dans la configuration du périphérique. Vous verrez la commande curl, le corps de la réponse et le code de réponse. Si vous avez créé un corps valide, vous devriez voir **200** dans le champ **Response Code** (Code de réponse).

Si vous avez fait une erreur, consultez le corps de la réponse pour obtenir un message d'erreur. Vous pouvez corriger la valeur du corps et réessayer.

h) Revenez à Gestionnaire de périphériques de pare-feu en cliquant sur **Device** (Périphérique) dans le menu supérieur.

i) Cliquez sur **Objects** (Objets), puis sur **Identity Sources** (Sources d'identité) dans la table des matières.

Votre objet Duo LDAP devrait apparaître dans la liste. Si ce n'est pas le cas, retournez à API Explorer (Explorateur API) et essayez de créer l'objet de nouveau. Vous pouvez utiliser la méthode GET pour vérifier s'il a bien été créé.

Notez que vous pouvez supprimer l'objet à l'aide de Gestionnaire de périphériques de pare-feu, mais que vous ne pouvez pas le modifier ou voir son contenu. Vous devez utiliser l'API pour ces actions. Les méthodes pertinentes sont affichées dans le groupe **DuoLDAPIdentitySource**.

Étape 3 Chargez le certificat d'autorité de certification approuvé pour le site Web Duo dans Gestionnaire de périphériques de pare-feu.

Le système Firewall Threat Defense doit disposer du certificat nécessaire pour valider la connexion au serveur Duo LDAP. Vous pouvez obtenir et charger le certificat en suivant cette procédure, qui a été effectuée avec le navigateur Google Chrome. Les étapes exactes peuvent varier selon votre navigateur. Vous pouvez également accéder directement à https://www.digicert.com/digicert-root-certificates.htm et télécharger le certificat, mais la procédure suivante est générique et vous pouvez l'utiliser pour obtenir des certificats d'autorité de certification racine approuvés pour n'importe quel site.

a) Ouvrez https://duo.com dans votre navigateur.

b) Cliquez sur le lien d'information du site dans le champ URL du navigateur, puis sur le lien **Certificate** (Certificat). Cette action ouvre la boîte de dialogue d'informations sur le certificat.

c) Cliquez sur l'onglet **Certificate Path** (Chemin du certificat) et sélectionnez le niveau racine (supérieur) du chemin. Dans ce cas, DigiCert.

d) Une fois DigiCert sélectionné, cliquez sur **Afficher le certificat**. Cette action ouvrira une nouvelle boîte de dialogue de certificat, et l'onglet Général devrait indiquer qu'il a été émis pour l'autorité de certification racine EV de DigiCert High Assurance. Il s'agit du certificat de l'autorité de certification racine que vous devez charger dans Gestionnaire de périphériques de pare-feu.

e) Cliquez sur l'onglet **Details** (Détails), puis sur le bouton **Copy to File** (Copier dans un fichier) pour lancer l'assistant de téléchargement de certificat.

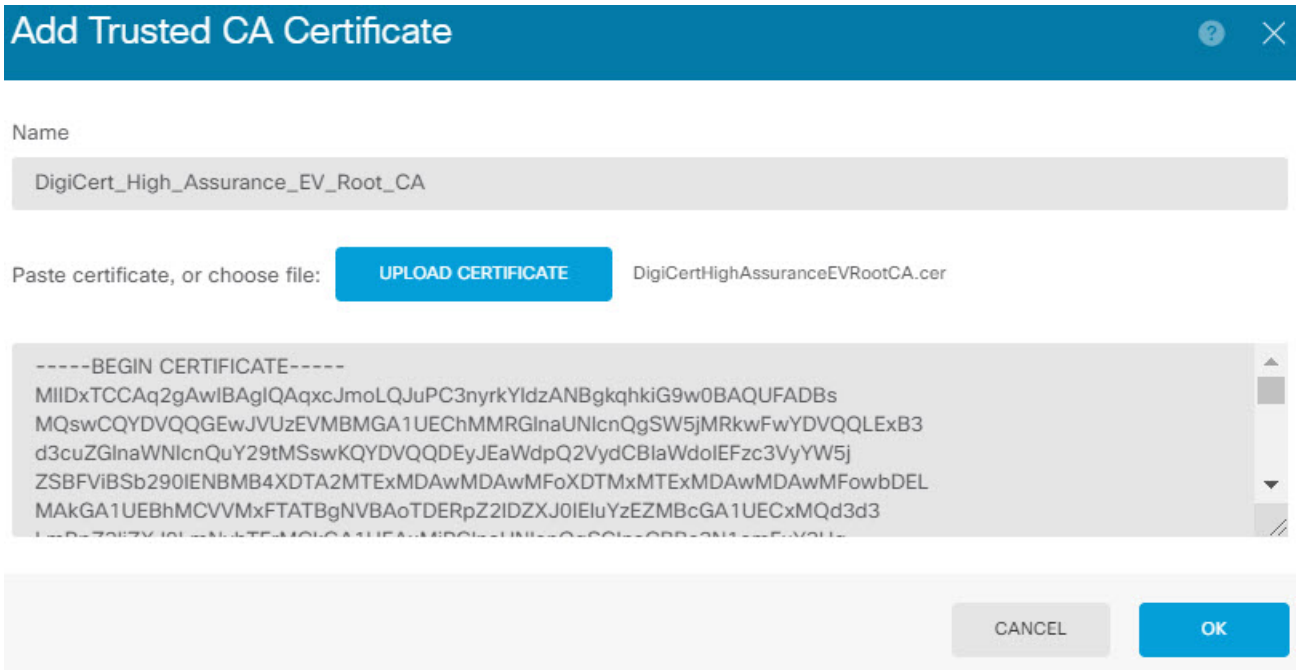
f) Utilisez l'assistant pour télécharger le certificat sur votre poste de travail. Téléchargez au format DER par défaut.

g) Dans la liste Gestionnaire de périphériques de pare-feu, choisissez **Objects** > **(Objets)** > **Certificates** (Certificats) .

h) Cliquez sur **+** > **Add Trusted CA Certificate** (Ajouter un certificat d'autorité de certification de confiance).

i) Saisissez un nom pour le certificat, par exemple, DigiCert_High_Assurance_EV_Root_CA. (Les espaces ne sont pas autorisés.)

j) Cliquez sur **Upload Certificate** (Charger le certificat) et sélectionnez le fichier que vous avez téléchargé.



k) Cliquez sur **OK**.

Étape 4 Utilisez l'éditeur de profil client AnyConnect pour créer un profil qui spécifie 60 secondes ou plus pour le délai d'authentification.

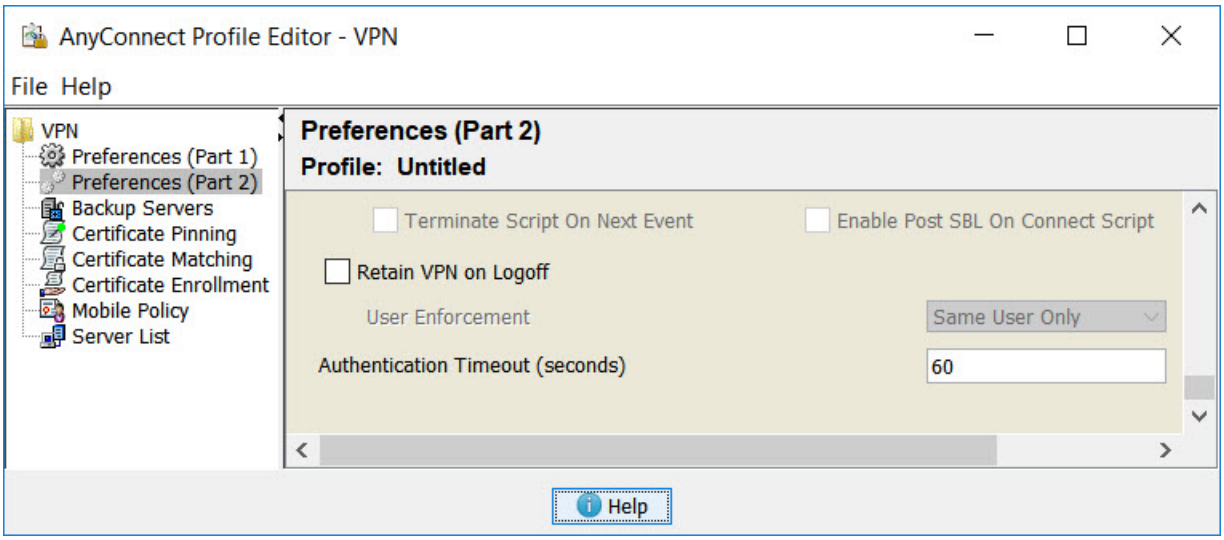
Vous devez accorder aux utilisateurs un délai supplémentaire pour obtenir le code d'accès Duo et effectuer l'authentification secondaire. Nous recommandons au moins 60 secondes.

Pour en savoir plus sur la création de profils client AnyConnect et leur téléchargement, consultez Configurer et charger les profils client AnyConnect, à la page 713. La procédure suivante explique comment configurer le délai d'authentification uniquement, puis charger le profil dans Firewall Threat Defense. Si vous souhaitez modifier d'autres paramètres, vous pouvez le faire maintenant.

a) Si vous ne l'avez pas encore fait, téléchargez et installez le progiciel de l'éditeur de profil client AnyConnect. Vous pouvez le trouver dans le centre de logiciels Cisco (software.cisco.com), dans le dossier correspondant à votre version client AnyConnect.

b) Ouvrez le **VPN Profile Editor (Éditeur de profil VPN)** client AnyConnect.

c) Sélectionnez **Preferences (Part 2)** (Préférences (Partie 2)) dans la table des matières, faites défiler jusqu'à la fin de la page et modifiez **Authentication Timeout** (Délai d'authentification) à 60 (ou plus). L'image suivante provient de l'éditeur de profil VPN AnyConnect 4.7 ; les versions précédentes ou ultérieures peuvent être différentes.



d) Choisissez **File (Fichier)** > **Save (Enregistrer)**, puis enregistrez le fichier XML de profil sur votre poste de travail avec un nom approprié, par exemple « duo-ldap-profile.xml ».

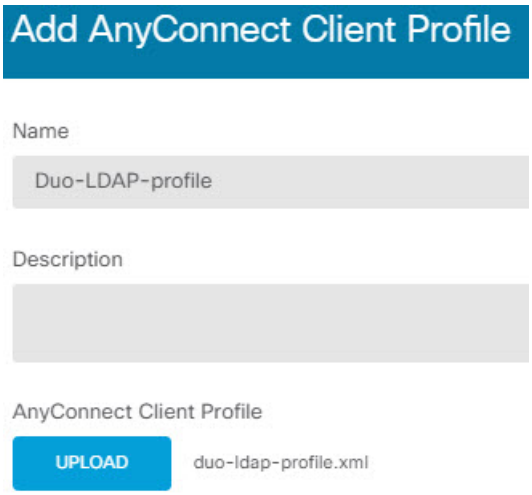
Vous pouvez maintenant fermer l'application de l'éditeur de profil VPN.

e) Dans Gestionnaire de périphériques de pare-feu, choisissez **Objects (Objets)** > **AnyConnect Client Profiles (Profils client AnyConnect)**.

f) Cliquez sur **+** pour créer un nouvel objet de profil.

g) Saisissez un **Name** (Nom) pour l'objet. Par exemple, Duo-LDAP-profile.

h) Cliquez sur **Upload** (Charger), et sélectionnez le fichier XML que vous avez créé.



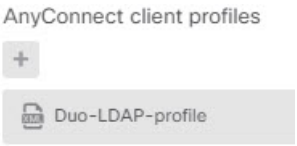
i) Cliquez sur **OK**.

Étape 5 Créez une politique de groupe et sélectionnez le profil client AnyConnect dans la politique.

La politique de groupe que vous affectez à un utilisateur contrôle de nombreux aspects de la connexion. La procédure suivante explique comment affecter le fichier XML de profil au groupe. Pour plus de détails sur ce que vous pouvez faire avec les politiques de groupe, consultez Configurer les politiques de groupe pour le VPN d'accès à distance, à la page 726.

a) Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)**.
b) Choisissez **Group Policies** (Politiques de groupe) dans la table des matières.
c) Modifiez DfltGrpPolicy, ou cliquez sur + et créez une nouvelle politique de groupe. Par exemple, si vous avez besoin d'un profil de connexion VPN d'accès à distance unique pour tous les utilisateurs, la modification de la politique de groupe par défaut est appropriée.
d) Sur la page General (Général), configurez les propriétés suivantes :

- **Name** (Nom) : pour un nouveau profil, saisissez un nom. Par exemple, Duo-LDAP-group.
- **AnyConnect Client Profiles (Profils client AnyConnect)** : cliquez sur + et sélectionnez l'objet de profil client AnyConnect que vous avez créé.



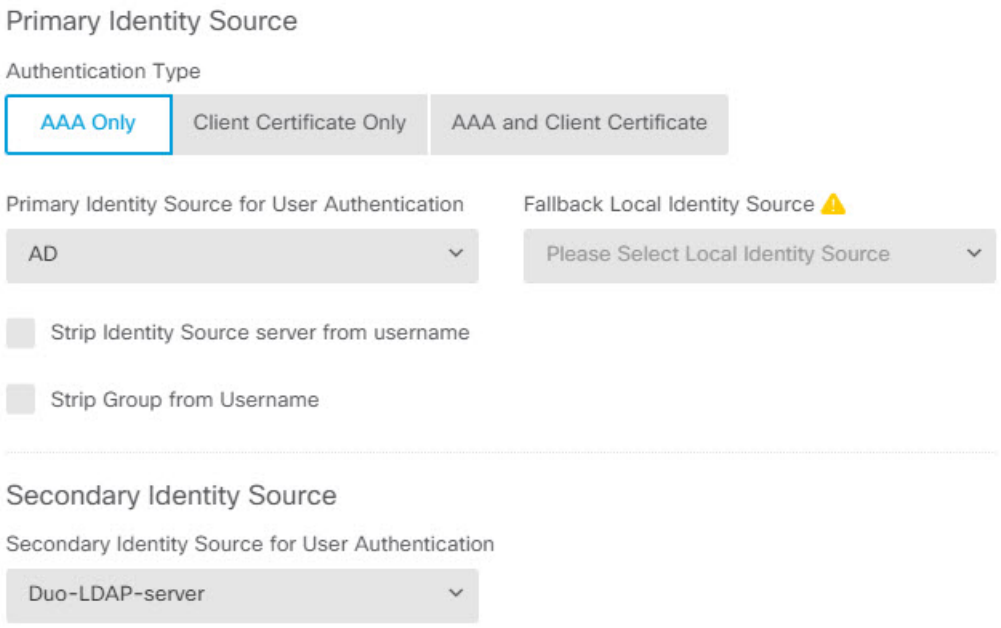
e) Cliquez sur **OK** pour enregistrer le profil de groupe.

Étape 6 Créez ou modifiez le profil de connexion VPN d'accès à distance à utiliser pour l'authentification secondaire Duo-LDAP.

Il y a plusieurs étapes à suivre pour configurer un profil de connexion, qui sont expliquées dans Configurer un profil de connexion VPN d'accès à distance, à la page 718. La procédure suivante ne mentionne que les modifications clés à apporter pour activer Duo-LDAP comme source d'authentification secondaire et pour appliquer le profil client AnyConnect. Pour les nouveaux profils de connexion, vous devez configurer le reste des champs obligatoires. Pour cette procédure, nous supposons que vous modifiez un profil de connexion existant, et vous devez simplement modifier ces deux paramètres.

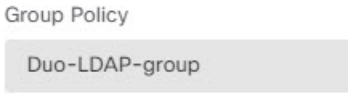
a) Sur la page RA VPN (VPN d'accès à distance), choisissez **Connection Profiles (Profils de connexion)** dans la table des matières.
b) Modifiez un profil de connexion existant ou créez-en un nouveau.
c) Sous Primary Identity Source (Source d'identité principale), configurez les éléments suivants :

- **Authentication Type** (Type d'authentification) : choisissez **AAA Only** (AAA uniquement) ou **AAA and Client Certificate** (AAA et certificat client). Vous ne pouvez pas configurer l'authentification à deux facteurs, sauf si vous utilisez AAA.
- **Primary Identity Source for User Authentication** (Source d'identité principale pour l'authentification des utilisateurs) : sélectionnez votre serveur Active Directory ou RADIUS principal. Notez que vous pouvez sélectionner une source d'identité Duo-LDAP comme source principale. Cependant, Duo-LDAP fournit des services d'authentification uniquement, et non des services d'identité, donc si vous l'utilisez comme source d'authentification principale, vous ne verrez pas les noms d'utilisateur associés aux connexions VPN d'accès à distance dans les tableaux de bord, et vous ne pourrez pas écrire de règles de contrôle d'accès pour ces utilisateurs. (Vous pouvez configurer le retour à la source d'identité locale si vous le souhaitez.)
- **Secondary Identity Source** (Source d'identité secondaire) : sélectionnez la source d'identité Duo-LDAP.



d) Cliquez sur **Next** (suivant).

e) Sur la page Remote User Experience (Expérience de l'utilisateur à distance), sélectionnez la **Group Policy** (Politique de groupe) que vous avez créée ou modifiée.



f) Cliquez sur **Next (Suivant)** sur cette page et sur la page suivante, Global Settings (Paramètres globaux).

g) Cliquez sur **Finish** (Terminer) pour enregistrer vos modifications du profil de connexion.

Étape 7 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

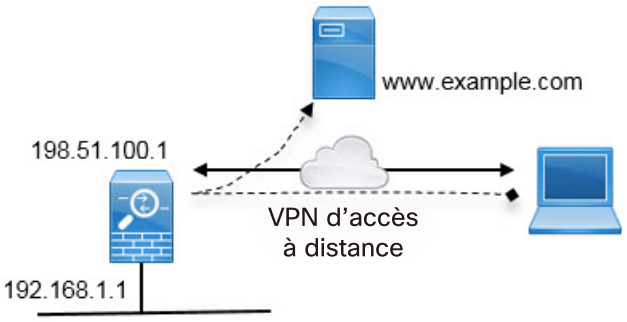
Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Comment fournir un accès Internet sur l'interface externe pour les utilisateurs du VPN d'accès à distance (Hair Pinning)

En règle générale, dans le VPN d'accès à distance, vous pouvez souhaiter que les utilisateurs du VPN accèdent à Internet par l'intermédiaire de votre périphérique. Cependant, comme les utilisateurs distants accèdent à

votre périphérique sur la même interface qui fait face à Internet (l'interface externe), vous devez faire revenir le trafic Internet directement sur l'interface externe. Cette technique est appelée hairpinning.

Le graphique suivant présente un exemple. Un VPN d'accès à distance est configuré sur l'interface externe, 198.51.100.1. Vous souhaitez fractionner le tunnel VPN de l'utilisateur distant, de sorte que le trafic Internet soit renvoyé par l'interface externe, tandis que le trafic vers vos réseaux internes continue par le périphérique. Ainsi, lorsqu'un utilisateur distant souhaite accéder à un serveur sur Internet, comme par exemple www.exemple.com, la connexion passe d'abord par le VPN, puis est acheminée vers l'Internet à partir de l'interface 198.51.100.1.



La procédure suivante explique comment configurer ce service.

Avant de commencer

Cet exemple suppose que vous avez déjà enregistré le périphérique, appliqué une licence VPN d'accès à distance et téléchargé l'image client AnyConnect. Il suppose également que vous ayez configuré le domaine d'identité, qui est également utilisé dans les politiques d'identité.

Procédure

Étape 1 Configurez la connexion VPN d'accès à distance.

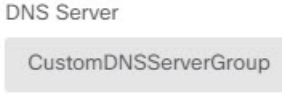
La configuration nécessite une politique de groupe personnalisée en plus du profil de connexion. Étant donné que le hairpinning est une configuration courante et que les paramètres requis dans la politique de groupe sont généralement applicables, dans cet exemple, nous modifierons la politique de groupe par défaut au lieu de créer une nouvelle politique de groupe. Vous pouvez adopter l'une ou l'autre des approches.

a) Cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance**.

b) Cliquez sur **Group Policies** (Politiques de groupe) dans la table des matières, puis sur l'icône de modification ( ) de l'objet DfltGrpPolicy.

c) Apportez les modifications suivantes à la politique de groupe par défaut :

- Sur la page **General** (Général), dans **DNS Server** (Serveur DNS), sélectionnez le groupe de serveurs DNS qui définit les serveurs que les points d'extrémité VPN doivent utiliser pour résoudre les noms de domaine.



- Sur la page **Split Tunneling** (Tunnellisation fractionnée), pour **IPv4 Split Tunneling** (Tunnellisation fractionnée IPv4) et **IPv6 Split Tunneling** (Tunnellisation fractionnée IPv6), sélectionnez l'option **Allow all traffic over tunnel** (Autoriser tout le trafic sur le tunnel). Il s'agit du paramètre par défaut, il est donc peut-être déjà configuré correctement.



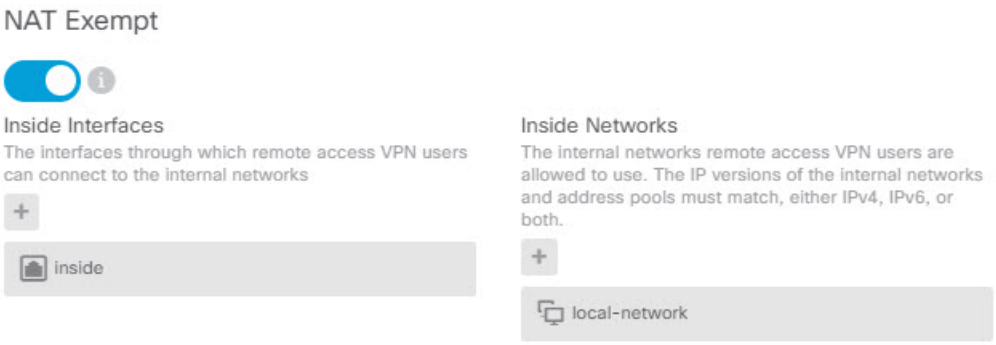
Remarque
Il s'agit d'un paramètre critique pour activer le hair-pinning. Vous souhaitez que tout le trafic atteigne la passerelle VPN, alors que la tunnellisation fractionnée est un moyen de permettre aux clients distants d'accéder directement aux sites locaux ou Internet en dehors du VPN.

d) Cliquez sur **OK** pour enregistrer les modifications apportées à la politique de groupe par défaut.
e) Cliquez sur **Connection Profiles** (Profils de connexion) et modifiez un profil existant ou créez-en un nouveau.
f) Dans le profil de connexion, parcourez l'assistant et configurez toutes les options comme vous le feriez pour toute autre configuration de VPN d'accès à distance. Cependant, vous devez configurer correctement les options suivantes pour activer le hair-pinning :

- **Group Policy** (Politique de groupe), à l'étape 2. Sélectionnez la politique de groupe que vous avez personnalisée pour le hairpinning.



- **NAT Exempt (Exemption de NAT)**, à l'étape 3. Activez cette fonctionnalité. Sélectionnez l'interface interne, puis sélectionnez un objet réseau qui définit les réseaux internes. Dans cet exemple, l'objet doit préciser 192.168.1.0/24. Le trafic VPN d'accès à distance vers le réseau interne ne recevra pas de traduction d'adresses. Cependant, comme le trafic hair-pinned passe par l'interface externe, il sera toujours transmis à l'aide de la NAT, car l'exemption NAT s'applique uniquement à l'interface interne. Notez que si d'autres profils de connexion sont définis, vous devez ajouter aux paramètres existants, car la configuration s'applique à tous les profils de connexion.



Remarque
L'option **NAT Exempt** (Exemption de NAT) est l'autre paramètre critique pour la configuration de hairpinning.

g) (Facultatif) Dans l'étape **Global Settings** (Paramètres globaux), sélectionnez l'option **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)** (Contourner la stratégie de contrôle d'accès pour le trafic déchiffré).

En sélectionnant cette option, vous n'avez plus besoin de configurer des règles de contrôle d'accès pour autoriser le trafic provenant des adresses du pool du VPN d'accès à distance (RA). Cette option améliore la sécurité (les utilisateurs externes ne peuvent pas usurper les adresses du pool), mais elle signifie que le trafic du VPN d'accès à distance (RA) est exempt d'inspection, y compris le filtrage d'URL et la protection contre les intrusions. Pesez le pour et le contre avant de choisir cette option.

h) Passez en revue la configuration du VPN d'accès à distance, puis cliquez sur **Finish** (Terminer).

Étape 2 Configurez la règle NAT pour traduire toutes les connexions sortant de l'interface externe en ports sur l'adresse IP externe (PAT de l'interface).

Lorsque vous avez terminé la configuration initiale du périphérique, le système crée une règle NAT nommée InsideOutsideNatRule. Cette règle applique la PAT d'interface au trafic IPv4 de toute interface qui quitte le périphérique par l'intermédiaire de l'interface externe. Comme l'interface externe est incluse dans l'interface source « Any », la règle dont vous avez besoin existe déjà, sauf si vous l'avez modifiée ou supprimée.

La procédure suivante explique comment créer la règle dont vous avez besoin.

a) Cliquez sur **Policies (Politiques)** > **NAT**.

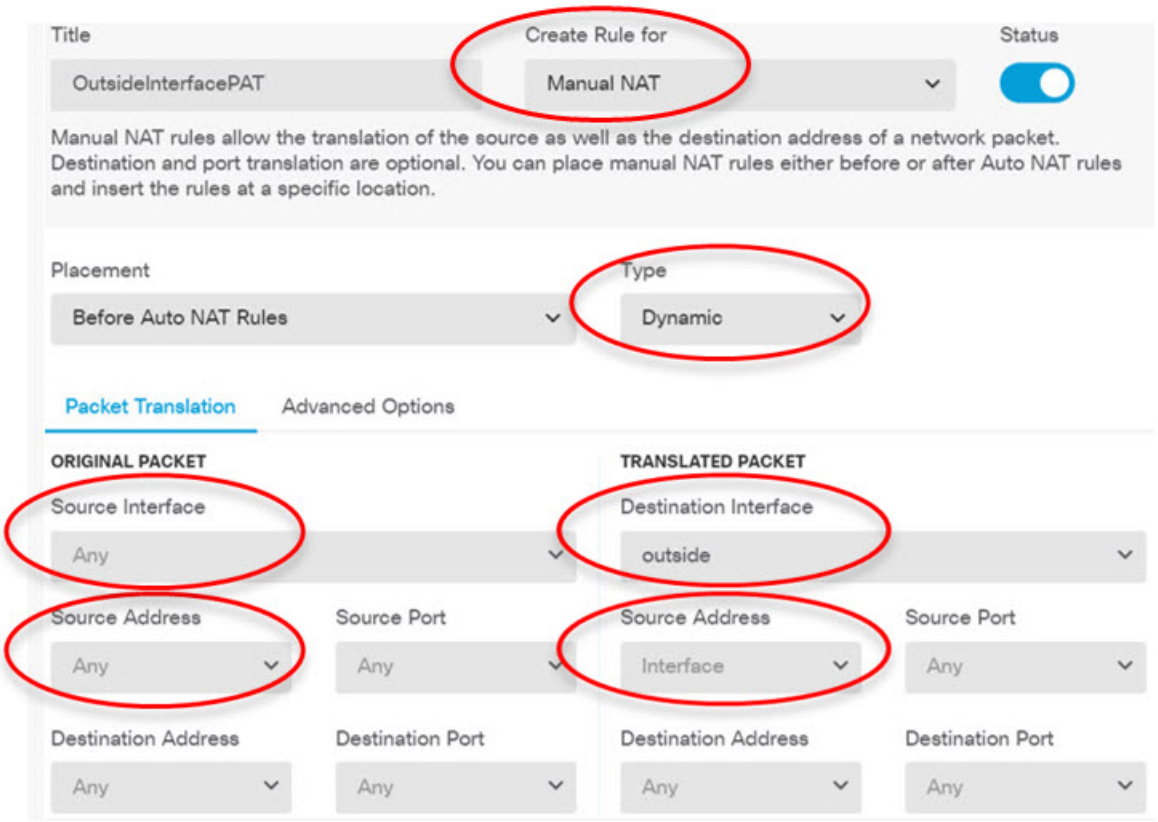
b) Effectuez l'une des opérations suivantes :

- Pour modifier la règle InsideOutsideNatRule, passez le curseur sur la colonne **Action** et cliquez sur l'icône de modification ().
- Pour créer une nouvelle règle, cliquez sur le bouton **+**.

c) Configurez une règle avec les propriétés suivantes :

- **Title** (Titre) : pour une nouvelle règle, saisissez un nom significatif, sans espaces. Par exemple, OutsideInterfacePAT.
- **Create Rule For** (Créer une règle pour) : **Manual NAT** (NAT manuelle).
- **Placement** : **Before Auto NAT Rules (Avant les règles de NAT automatique)** (valeur par défaut).
- **Type** :**Dynamic** (Dynamique).
- **Original Packet** (Paquet d'origine) : pour **Source Address** (Adresse source), sélectionnez Any (tout) ou any-ipv4. Pour **Source Interface** (Interface source), veillez à sélectionner Any (tout) (qui est la valeur par défaut). Pour toutes les autres options de Original Packet (Paquet d'origine), conservez la valeur par défaut, Any (tout).
- **Translated Packet** (Paquet traduit) : pour **Destination Interface** (Interface de destination), sélectionnez externe. Pour **Translated Address** (Adresse traduite), sélectionnez **Interface**. Pour toutes les autres options de Translated Packet (Paquet traduit), conservez la valeur par défaut, Any (tout).

Le graphique suivant montre le cas simple où vous sélectionnez Any (tout) pour l'adresse source.



d) Cliquez sur **OK**.

Étape 3 (Si vous ne configurez pas **Bypass Access Control policy for decrypted traffic** (sysopt permit-vpn) (stratégie de contrôle d'accès de contournement pour le trafic déchiffré) dans le profil de connexion.) Créez des règles de contrôle d'accès pour autoriser l'accès à partir de l'ensemble d'adresses VPN d'accès à distance.

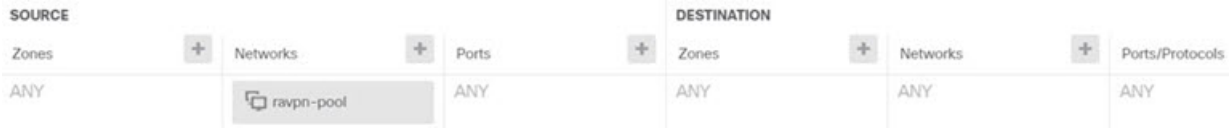
Si vous sélectionnez **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)** (stratégie de contrôle d'accès de contournement pour le trafic déchiffré) dans le profil de connexion, le trafic de l'ensemble d'adresses du VPN d'accès à distance contourne la stratégie de contrôle d'accès. Vous ne pouvez pas écrire de règles de contrôle d'accès qui s'appliqueront au trafic. Vous devez écrire les règles uniquement si vous désactivez l'option.

L'exemple suivant permet le trafic de l'ensemble d'adresses vers n'importe quelle destination. Vous pouvez l'ajuster selon vos besoins précis. Vous pouvez également faire précéder la règle de règles de blocage pour filtrer le trafic indésirable.

a) Cliquez sur **Policies (Politiques)** > **Access Control (Contrôle d'accès)**.
b) Cliquez sur **+** pour créer une nouvelle règle.
c) Configurez une règle avec les propriétés suivantes :

- **Order** (Ordre) : sélectionnez une position dans la politique avant toute autre règle qui pourrait correspondre à ces connexions et les bloquer. La valeur par défaut consiste à ajouter la règle à la fin de la politique. Si vous devez repositionner la règle ultérieurement, vous pouvez modifier cette option ou simplement faire glisser et déposer la règle dans le bon emplacement dans le tableau.
- **Titre** : saisissez un nom significatif sans espaces. Par exemple, RAVPN-address-pool.

- **Action** : **Autoriser**. Vous pouvez sélectionner Trust (Confiance) si vous ne souhaitez pas que ce trafic soit inspecté pour détecter des violations de protocole ou des intrusions.
- Onglet **Source/Destination** : pour **Source** > **Network (Réseau)**, sélectionnez le même objet que vous avez utilisé dans le profil de connexion VPN d'accès à distance pour l'ensemble d'adresses. Laissez la valeur par défaut, Any (Tout), pour toutes les autres options de source et de destination.



- Onglets **Application**, **URL** et **Users** (Utilisateurs) : laissez les paramètres par défaut sur ces onglets, c'est-à-dire qu'aucune option n'est sélectionnée.
- Onglets **Intrusion**, **File** (Fichiers) : vous pouvez, au besoin, sélectionner des politiques de prévention des intrusions ou des politiques de fichiers afin d'inspecter les menaces ou les logiciels malveillants.
- Onglet**Logging (journalisation**) : vous pouvez éventuellement activer la journalisation des connexions.

d) Cliquez sur **OK**.

Étape 4 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

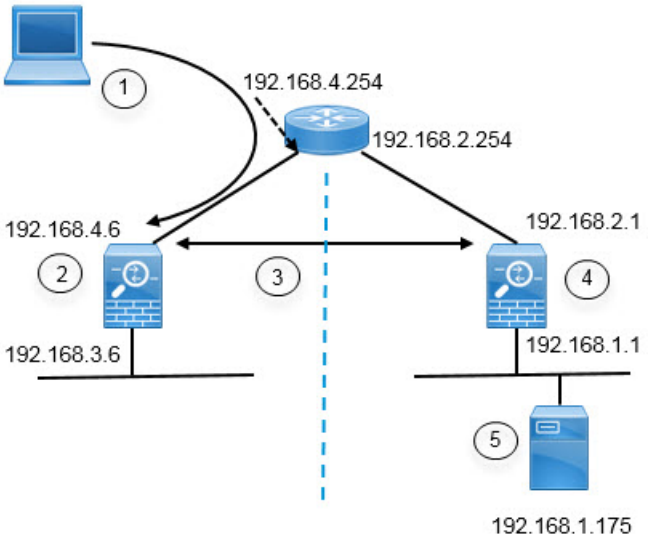
Comment utiliser un serveur de répertoire sur un réseau externe avec le VPN d'accès à distance

Vous pouvez configurer un VPN d'accès à distance pour permettre aux télétravailleurs et aux télétravailleurs de se connecter en toute sécurité à vos réseaux internes. La sécurité de la connexion dépend de votre serveur de répertoire, qui authentifie la connexion de l'utilisateur pour s'assurer que seuls les utilisateurs autorisés peuvent obtenir l'entrée.

Si votre serveur de répertoire se trouve sur un réseau externe plutôt que sur un réseau interne, vous devez configurer une connexion VPN de site à site à partir de l'interface externe vers le réseau qui comprend le serveur de répertoire. **Il existe une optimisation de la configuration VPN de site à site :** vous devez inclure l'adresse de l'interface externe du périphérique VPN d'accès à distance dans les réseaux « internes » de la connexion VPN de site à site, ainsi que dans les réseaux distants pour le périphérique derrière lequel se trouve le serveur de répertoire. Cela sera expliqué plus en détail dans la procédure suivante.

Remarque Si vous utilisez les interfaces de données comme passerelle pour l'interface de gestion virtuelle, cette configuration permet également l'utilisation du répertoire pour les politiques d'identité. Si vous n'utilisez pas d'interfaces de données comme passerelle de gestion, assurez-vous qu'il existe une voie de routage entre le réseau de gestion et le réseau interne qui participe à la connexion VPN de site à site.

Ce scénario d'utilisation met en œuvre le scénario réseau suivant.



Appel de la figure	Description
1	Hôte d'accès à distance qui établit une connexion VPN avec l'adresse 192.168.4.6. Les clients obtiendront une adresse dans l'ensemble d'adresses 172.18.1.0/24.
2	Le site A, qui héberge le VPN d'accès à distance.
3	Le tunnel VPN de site à site entre les interfaces externes du site A et du site B, pour les périphériques Firepower Threat Defense.
4	Le site B, qui héberge le serveur de répertoire.
5	Le serveur de répertoire, sur le réseau interne du site B.

Avant de commencer

Ce scénario suppose que vous ayez suivi l'assistant de configuration du périphérique pour établir une configuration de référence normale. Plus précisément :

- Il existe une règle de contrôle d'accès Inside_Outside_Rule qui autorise (ou fait confiance) le trafic passant de la zone interne à la zone externe.
- Les zones de sécurité inside_zone et outside_zone contiennent respectivement les interfaces interne et externe.

- Il existe une règle InsideOutsideNATRule qui effectue une PAT d'interface pour tout le trafic provenant des interfaces internes vers l'interface externe. Sur les périphériques qui utilisent un groupe de ponts internes par défaut, il peut y avoir plusieurs règles pour la PAT de l'interface.
- Il existe une route IPv4 statique pour 0.0.0.0/0 qui pointe vers l'interface externe. Cet exemple suppose que vous utilisez des adresses IP statiques pour les interfaces externes, mais vous pouvez également utiliser DHCP et obtenir la route statique de manière dynamique. Pour cet exemple, nous supposons les routes statiques suivantes :
  - Site A : interface externe, la passerelle est 192.168.4.254.
  - Site B : interface externe, la passerelle est 192.168.2.254.

Procédure

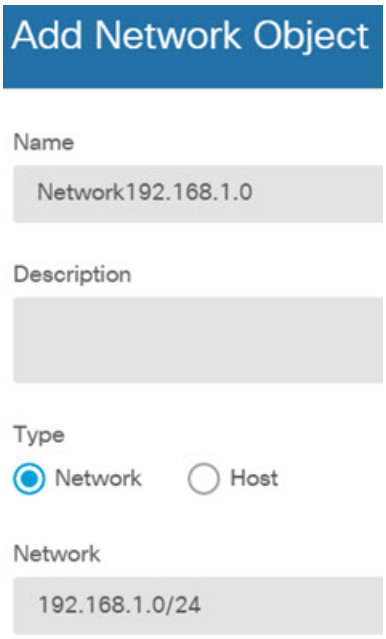
Étape 1 Configurez la connexion VPN de site à site sur **le site B**, qui héberge le serveur de répertoire.

a) Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le groupe Connexion VPN de site à site.

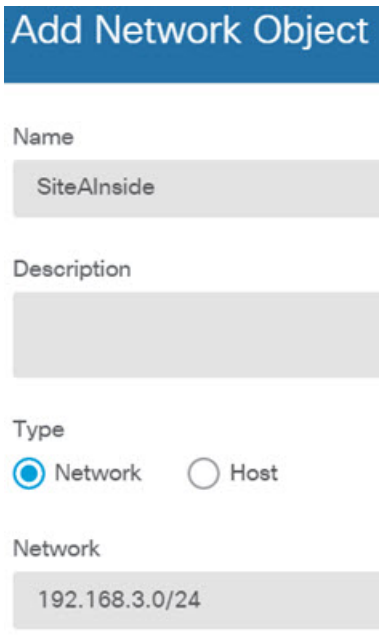
b) Cliquez sur le bouton **+**.

c) Configurez les options suivantes pour **Endpoint Setting**s (Paramètres de point terminal).

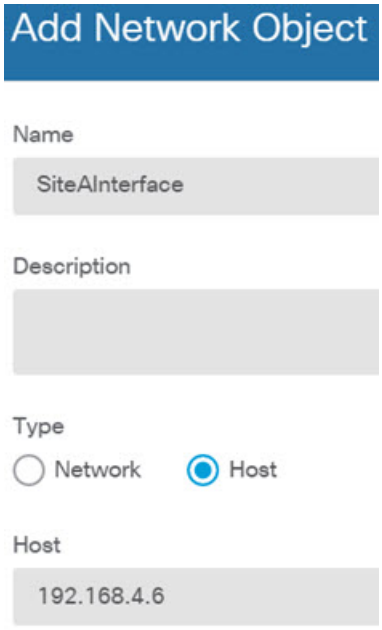
- **Connection Profile Name** (Nom du profil de connexion) : saisissez un nom, par exemple, SiteA (pour indiquer que la connexion se fait au site A).
- **Local Site** (site local) : ces options définissent le point terminal local.
  - **Local VPN Access Interface** (Interface d'accès VPN local) : sélectionnez l'interface **externe** (celle dont l'adresse 192.168.2.1 dans le diagramme).
  - **Local Network** (Réseau local) : cliquez sur le signe plus **+** et sélectionnez l'objet réseau qui identifie le réseau local qui doit faire partie de la connexion VPN. Comme le serveur de répertoire se trouve sur ce réseau, il peut participer au VPN de site à site. En supposant que l'objet n'existe pas déjà, cliquez sur **Create New Network** (Créer un nouveau réseau) et configurez un objet pour le réseau 192.168.1.0/24. Après avoir enregistré l'objet, sélectionnez-le dans la liste déroulante et cliquez sur **OK**.



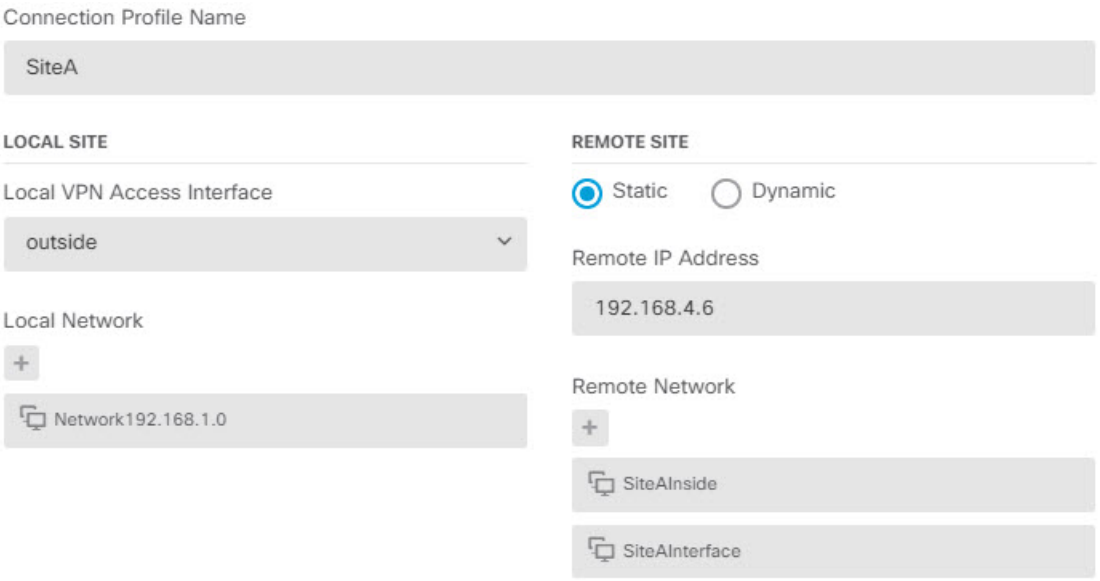
- **Remote Site** (Site distant) : ces options définissent le terminal distant.
  - **Remote IP Address** (Adresse IP distante) : saisissez 192.168.4.6, qui correspond à l'adresse IP de l'interface de l'homologue VPN distant qui hébergera la connexion VPN.
  - **Remote Networ**k (Réseau distant) : cliquez sur signe plus + et sélectionnez les objets réseau qui identifient les réseaux distants devant participer à la connexion VPN. Cliquez sur **Create New Network** (Créer un nouveau réseau), configurez les objets suivants, puis sélectionnez-les dans la liste.
    1. SiteAInside, réseau, 192.168.3.0/24.



2. SiteAInterface, hôte, 192.168.4.6. **Il s'agit de la clé : vous devez inclure l'adresse du point de connexion VPN d'accès à distance dans le cadre du réseau distant pour la connexion VPN de site à site afin que le VPN d'accès à distance hébergé sur cette interface puisse utiliser le serveur de répertoire.**



Lorsque vous avez terminé, les paramètres du terminal devraient ressembler à ce qui suit :



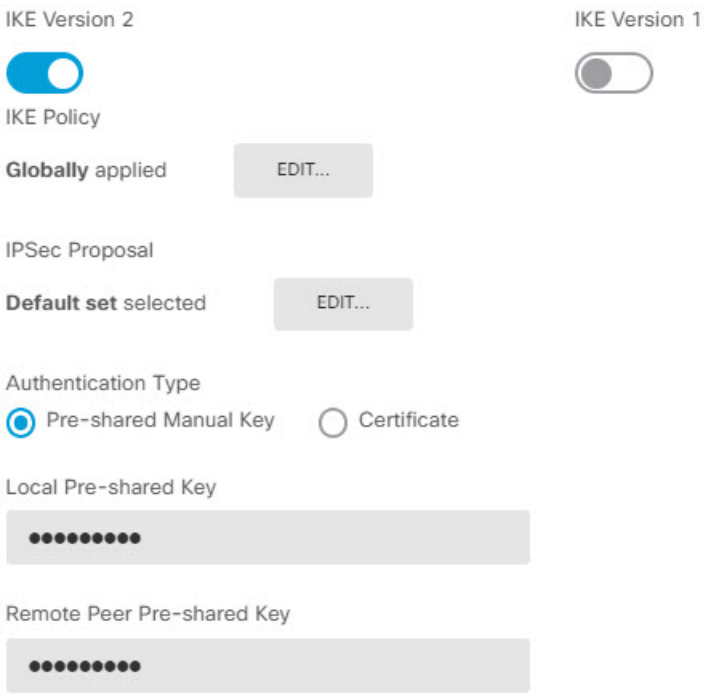
d) Cliquez sur **Next** (suivant).

e) Définissez la configuration de confidentialité pour le VPN.

Dans ce cas d'utilisation, nous supposons que vous êtes admissible aux fonctionnalités soumises à des restrictions d'exportation, ce qui permet l'utilisation d'un chiffrement renforcé. Ajustez ces exemples de paramètres en fonction de vos besoins et des exigences de votre licence.

- **IKE version 2**, **IKE version 1** : conservez les valeurs par défaut, **IKE version 2** activée, **IKE version 1** désactivée.
- **IKE Policy** (Politique IKE) : cliquez sur **Edit** (Modifier) et activez **AES-GCM-NULL-SHA** et **AES-SHA-SHA**, et désactivez **DES-SHA-SHA**.
- **IPsec Proposal** (Proposition IPsec) : cliquez sur **Edit** (Modifier). Dans la boîte de dialogue Select IPSec Proposals (Sélectionner les propositions IPSec), cliquez sur le signe **+**, puis cliquez sur **Set Default** (Définir par défaut) pour choisir les propositions AES-GCM par défaut.
- **Local Preshared Key** (Clé prépartagée locale), **Remote Peer Preshared Key** (Clé prépartagée de l'homologue distant) : saisissez les clés définies sur ce périphérique et sur le périphérique distant pour la connexion VPN. Ces clés peuvent être différentes dans IKEv2. La clé peut comporter entre 1 et 127 caractères alphanumériques. **N'oubliez pas ces clés, car vous devez configurer les mêmes chaînes lors de la création de la connexion VPN de site à site sur le périphérique du site A.**

La politique IKE doit ressembler à ce qui suit :



f) Configurez les **options supplémentaires**.

- **NAT Exempt** (Exemption NAT : sélectionnez l'interface qui héberge le réseau interne, dans cet exemple, l'interface **interne**. En règle générale, vous ne souhaitez pas que le trafic dans un tunnel VPN de site à site voie les adresses IP traduites. Cette option ne fonctionne que si le réseau local se trouve derrière une interface de routage unique (et non un membre d'un groupe de ponts). Si le réseau local se trouve derrière plusieurs interfaces de routage ou un ou plusieurs membres de groupes de pont, vous devez créer manuellement les règles d'exemption NAT. Pour plus

d'informations sur la création manuelle des règles requises, consultez Exemption du trafic VPN de site à site de la NAT, à la page 685.

- **Diffie-Hellman Group for Perfect Forward Secrecy (Groupe Diffie-Hellman pour la confidentialité de transmission** parfaite) : sélectionnez **Group 19** (Groupe 19). Cette option détermine si l'on utilise la confidentialité de transmission parfaite (PFS) pour générer et utiliser une clé de session unique pour chaque échange chiffré. La clé de session unique protège l'échange du déchiffrement ultérieur, même si l'échange en entier a été enregistré et que l'agresseur a obtenu les clés prépartagées ou privées utilisées par les terminaux. Pour obtenir une explication des options, consultez Choix du groupe de module Diffie-Hellman à utiliser, à la page 662.

Les options doivent ressembler à ce qui suit.



g) Cliquez sur **Next** (suivant).

h) Passez en revue le résumé et cliquez sur **Finish** (Terminer).

Les renseignements récapitulatifs sont copiés dans le presse-papiers. Vous pouvez coller ces renseignements dans un document et les utiliser pour vous aider à configurer l'homologue distant ou les envoyer à la personne responsable de la configuration de cet homologue.

i) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



j) Cliquez sur le bouton **Deploy Now** (Déployer maintenant) et attendez la fin du déploiement.

Le périphérique du site B est maintenant prêt à héberger une extrémité de la connexion VPN de site à site.

Étape 2 Déconnectez-vous du périphérique **du site B** et connectez-vous au périphérique **du site A**.

Étape 3 Configurez la connexion VPN de site à site sur **le site A**, qui accueillera le VPN d'accès à distance.

a) Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le groupe Connexion VPN de site à site.

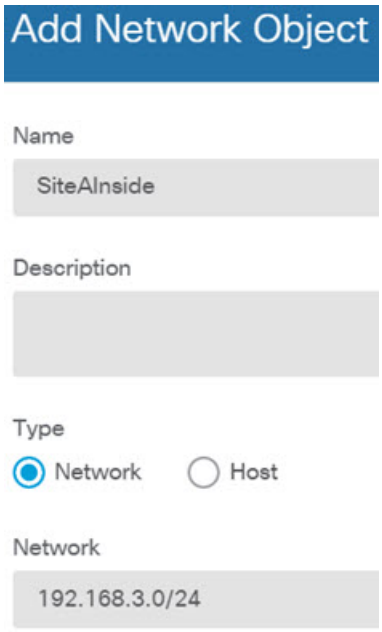
b) Cliquez sur le bouton +.

c) Configurez les options suivantes pour **Endpoint Setting**s (Paramètres de point terminal).

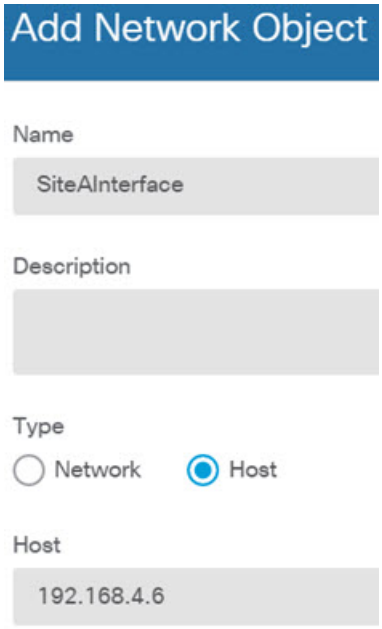
- **Connection Profile Name** (Nom du profil de connexion) : saisissez un nom, par exemple, SiteB (pour indiquer que la connexion se fait au site B).
- **Local Site** (Site local) : ces options définissent le point terminal local.
  - **Local VPN Access Interface** (Interface d'accès VPN local) : sélectionnez l'interface **externe** (celle dont l'adresse 192.168.4.6 dans le diagramme).
  - **Local Network** (Réseau local) : cliquez sur le signe plus + et sélectionnez les objets réseau qui identifient les réseaux locaux qui doivent participer à la connexion VPN. Cliquez sur

Create New Network (Créer un nouveau réseau), configurez les objets suivants, puis sélectionnez-les dans la liste. **Notez que vous avez créé les mêmes objets dans le périphérique du site B, mais que vous devez les créer à nouveau dans le périphérique du site A.**

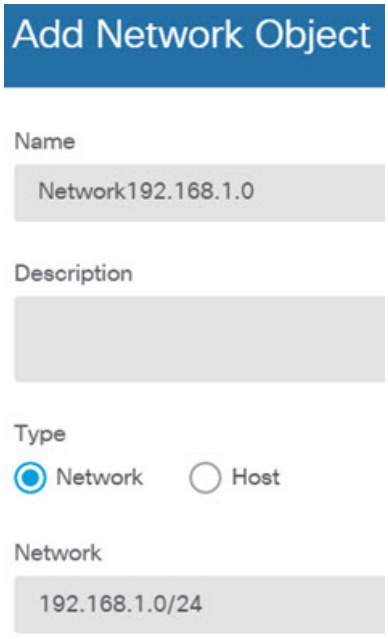
1. SiteAInside, réseau, 192.168.3.0/24.



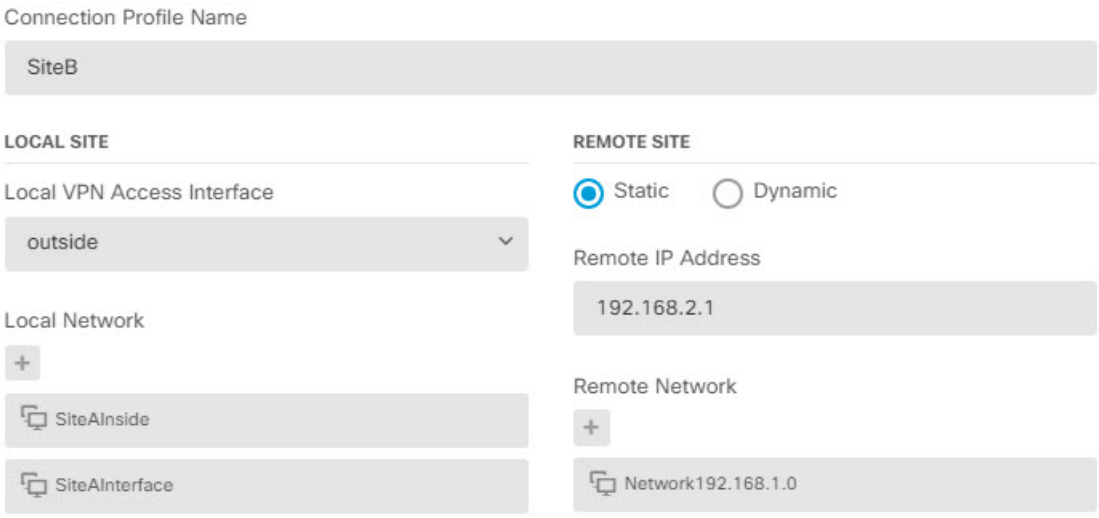
2. SiteAInterface, hôte, 192.168.4.6. **Il s'agit de la clé : vous devez inclure l'adresse du point de connexion VPN d'accès à distance en tant que partie du réseau interne pour la connexion VPN de site à site afin que le VPN d'accès à distance hébergé sur cette interface puisse utiliser le serveur de répertoire sur le réseau distant.**



- **Remote Site** (Site distant) : ces options définissent le terminal distant.
  - **Remote IP Address** (Adresse IP distante) : saisissez 192.168.2.1, qui correspond à l'adresse IP de l'interface de l'homologue VPN distant qui hébergera la connexion VPN.
  - **Remote Network** (Réseau distant) : cliquez sur le signe + et sélectionnez l'objet réseau qui identifie le réseau distant qui doit participer à la connexion VPN, celui qui comprend le serveur de répertoire. Cliquez sur **Create New Network** (Créer un nouveau réseau) et configurez un objet pour le réseau 192.168.1.0/24. Après avoir enregistré l'objet, sélectionnez-le dans la liste déroulante et cliquez sur **OK**. **Notez que vous avez créé le même objet dans le périphérique du site B, mais que vous devez le créer à nouveau dans le périphérique du site A.**



Lorsque vous avez terminé, les paramètres de terminal devraient ressembler à ce qui suit. Remarquez que les réseaux locaux/distants sont inversés par rapport aux paramètres du site B. C'est ainsi que les deux extrémités d'une connexion point à point doivent toujours ressembler.

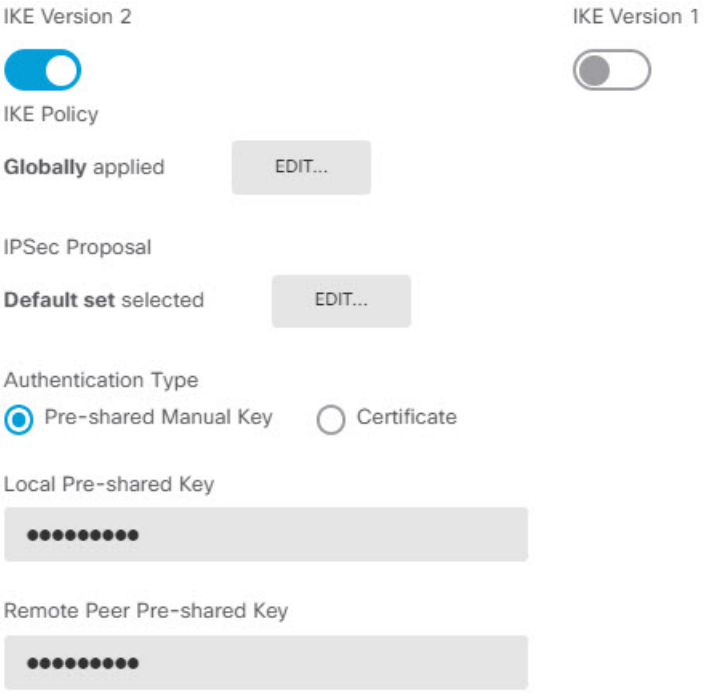


d) Cliquez sur **Next** (suivant).

e) Définissez la configuration de confidentialité pour le VPN.

Configurez la même version IKE, la même politique et la même proposition IPsec, et les mêmes clés prépartagées que vous l'avez fait pour la connexion au site B, **mais assurez-vous d'inverser les clés prépartagées Local et Remote**.

La politique IKE doit ressembler à ce qui suit :



f) Configurez les **options supplémentaires**.

- **NAT Exempt** (Exemption NAT : sélectionnez l'interface qui héberge le réseau interne, dans cet exemple, l'interface **interne**. En règle générale, vous ne souhaitez pas que le trafic dans un tunnel

VPN de site à site voie les adresses IP traduites. Cette option ne fonctionne que si le réseau local se trouve derrière une interface de routage unique (et non un membre d'un groupe de ponts). Si le réseau local se trouve derrière plusieurs interfaces de routage ou un ou plusieurs membres de groupes de pont, vous devez créer manuellement les règles d'exemption NAT. Pour plus d'informations sur la création manuelle des règles requises, consultez Exemption du trafic VPN de site à site de la NAT, à la page 685.

- **Diffie-Hellman Group for Perfect Forward Secrecy (Groupe Diffie-Hellman pour la confidentialité de transmission** parfaite) : sélectionnez **Group 19** (Groupe 19).

Les options doivent ressembler à ce qui suit.



g) Cliquez sur **Next** (suivant).
h) Passez en revue le résumé et cliquez sur **Finish** (Terminer).
i) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



j) Cliquez sur le bouton **Deploy Now** (Déployer maintenant) et attendez la fin du déploiement.

Le périphérique du site A est maintenant prêt à héberger l'autre extrémité de la connexion VPN de site à site. Comme le site B est déjà configuré avec des paramètres compatibles, les deux périphériques doivent négocier une connexion VPN.

Vous pouvez confirmer la connexion en vous connectant à l'interface de ligne de commande du périphérique et en envoyant un message ping au serveur de répertoire. Vous pouvez également utiliser la commande **show ipsec sa** pour afficher les informations de session.

Étape 4 Configurez le serveur de répertoire sur le **Site A**. Cliquez sur **Test** (Tester) pour vérifier qu'il y a une connexion.

a) Sélectionnez **Objects** (Objets), puis sélectionnez (Domaine d'identité) **Identity Sources** (Sources d'identité) dans la table des matières.
b) Cliquez sur **+** > **AD**.
c) Configurez les propriétés de base du domaine.

- **Name** (nom) : Nom du domaine de répertoire. Par exemple, AD.
- **Type** : Type de serveur d'annuaire. Active Directory est le seul type pris en charge et vous ne pouvez pas modifier ce champ.
- **Directory Username** (nom d'utilisateur), **Directory Password** (mot de passe d'annuaire) : nom d'utilisateur et mot de passe uniques pour un utilisateur disposant des droits appropriés sur les informations utilisateur que vous souhaitez récupérer. Pour Active Directory, l'utilisateur n'a pas besoin d'avoir des privilèges élevés. Vous pouvez préciser n'importe quel utilisateur dans le domaine. Le nom d'utilisateur doit être complet; par exemple, Administrateur@exemple.com (pas simplement Administrateur).

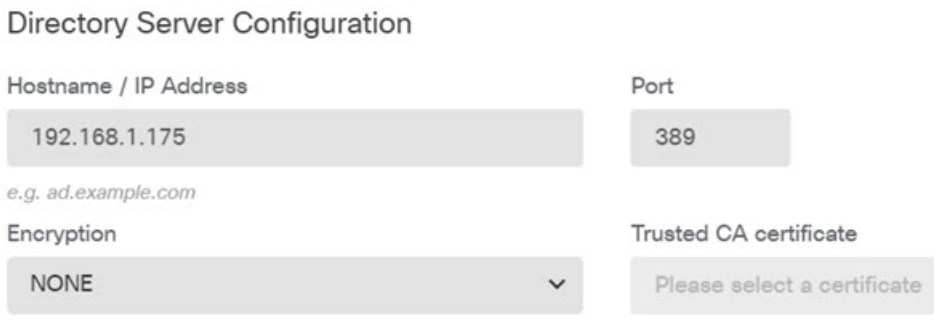
Remarque
Le système génère ldap-login-dn et ldap-login-password à partir de ces informations. Par exemple, Administrateur@exemple.com se traduit par cn=adminisntrator,cn=users,dc=example,dc=com. Notez que cn=users fait toujours partie de cette traduction; vous devez donc configurer l'utilisateur que vous précisez ici sous le nom usuel du dossier « users ».

- **Base DN** (base DN) : L'arborescence pour faire des recherches ou requêtes d'informations sur les utilisateurs et les groupes, c'est-à-dire le parent commun des utilisateurs et des groupes. Par exemple, cn=users,dc=example,dc=com. Pour en savoir plus sur la recherche du DN de base, consultez Détermination du DN de base du répertoire, à la page 170.
- **AD Primary Domain** (domaine principal AD) : le nom de domaine complet d'Active Directory que le périphérique doit joindre.' Par exemple, exemple.com.



d) Configurez les propriétés du serveur d'annuaire.

- **Hostname/IP Address** (nom d'hôte/adresse IP) : le nom d'hôte ou l'adresse IP du serveur d'annuaire. Si vous utilisez une connexion chiffrée avec le serveur, vous devez saisir le nom de domaine complet, et non l'adresse IP. Pour cet exemple, saisissez 192.168.1.175.
- **Port** : le numéro de port utilisé pour les communications avec le serveur. La valeur par défaut est 389. Utilisez le port 636 si vous sélectionnez LDAPS comme méthode de chiffrement. Pour cet exemple, conservez 389.
- **Encryption** (Chiffrement) : pour utiliser une connexion chiffrée afin de télécharger les informations sur les utilisateurs et les groupes. La valeur par défaut est **None** (aucun), ce qui signifie que les informations relatives aux utilisateurs et aux groupes sont téléchargées en texte en clair. Pour le VPN d'accès à distance, vous pouvez utiliser **LDAPS**, qui est LDAP sur SSL. Utilisez le port 636 si vous sélectionnez cette option. Le VPN d'accès à distance ne prend pas en charge STARTTLS. Pour cet exemple, sélectionnez **None** (Aucun).
- **Trusted CA Certificate** (certificat CA de confiance) : Si vous sélectionnez une méthode de chiffrement, téléchargez un certificat d'autorité de certification (CA) pour activer une connexion de confiance entre le système et le serveur d'annuaire. Si vous utilisez un certificat pour vous authentifier, le nom du serveur dans le certificat doit correspondre au nom d'hôte ou à l'adresse IP du serveur. Par exemple, si vous utilisez 192.168.1.175 comme adresse IP mais ad.exemple.com dans le certificat, la connexion échouera.



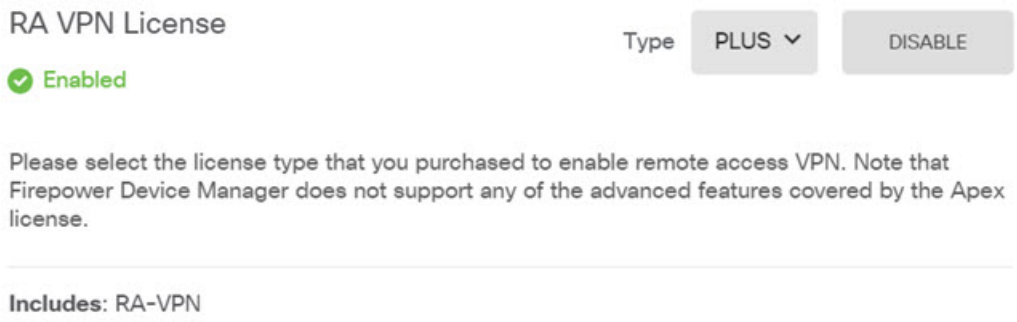
e) Cliquez sur le bouton **Test** (Tester) pour vérifier que le système peut communiquer avec le serveur.

Le système utilise des processus distincts pour accéder au serveur, de sorte que vous pourriez obtenir des erreurs indiquant que la connexion fonctionne pour un type d'utilisation mais pas pour un autre, par exemple, disponible pour les politiques d'identité mais pas pour le VPN d'accès à distance. Si le serveur n'est pas accessible, vérifiez que vous avez la bonne adresse IP et le bon nom d'hôte, que le serveur DNS dispose d'une entrée pour le nom d'hôte, etc. Vérifiez également que la connexion VPN de site à site fonctionne et que vous avez inclus l'adresse de l'interface externe du site A dans le VPN, et que la NAT ne traduit pas le trafic pour le serveur de répertoire. Vous devrez peut-être également configurer une route statique pour le serveur.

f) Cliquez sur **OK**.

Étape 5 Cliquez sur **Device (Périphérique)** > **Smart License (Licence Smart)** > **View Configuration (Afficher la configuration)**, et activez la licence de VPN d'accès à distance.

Lors de l'activation de la licence VPN d'accès à distance, sélectionnez le type de licence que vous avez acheté : Plus, Apex (ou les deux) ou VPN uniquement. Pour en savoir plus, consultez Exigences de licence pour le VPN d'accès à distance, à la page 710.

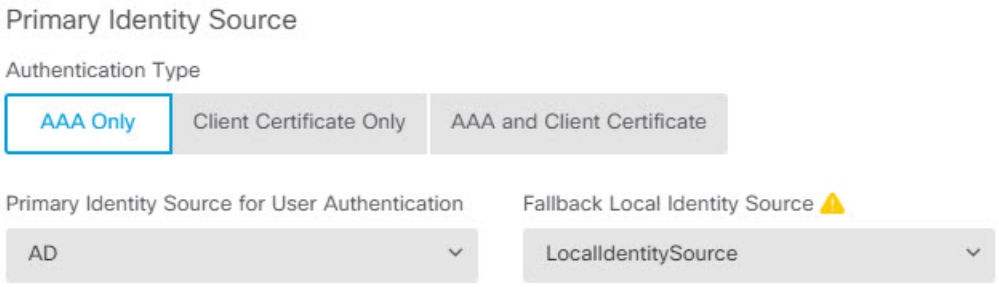


Étape 6 Configurez un VPN d'accès à distance sur le site A.

a) Cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance**. Assurez-vous que vous êtes sur la page **Connection Profiles** (Profils de connexion).

b) Créer ou modifier un profil de connexion.

c) Dans la première étape de l'assistant, configurez le nom de profil, puis sélectionnez le domaine AD comme source d'authentification principale. Vous pouvez éventuellement sélectionner la base de données locale comme source d'identité de repli.



d) Configurez l'ensemble d'adresses.

Pour cet exemple, cliquez sur **+**, puis sélectionnez **Create New Network** (Créer un nouveau réseau) dans l'ensemble d'adresses IPv4 et créez un objet pour le réseau 172.18.1.0/24, puis sélectionnez l'objet. Les clients reçoivent une adresse de cet ensemble. Laissez le champ IPv6 vide. L'ensemble d'adresses ne peut pas se trouver sur le même sous-réseau que l'adresse IP pour l'interface externe.

L'objet doit ressembler à ce qui suit :



La spécification de l'ensemble doit ressembler à ce qui suit :



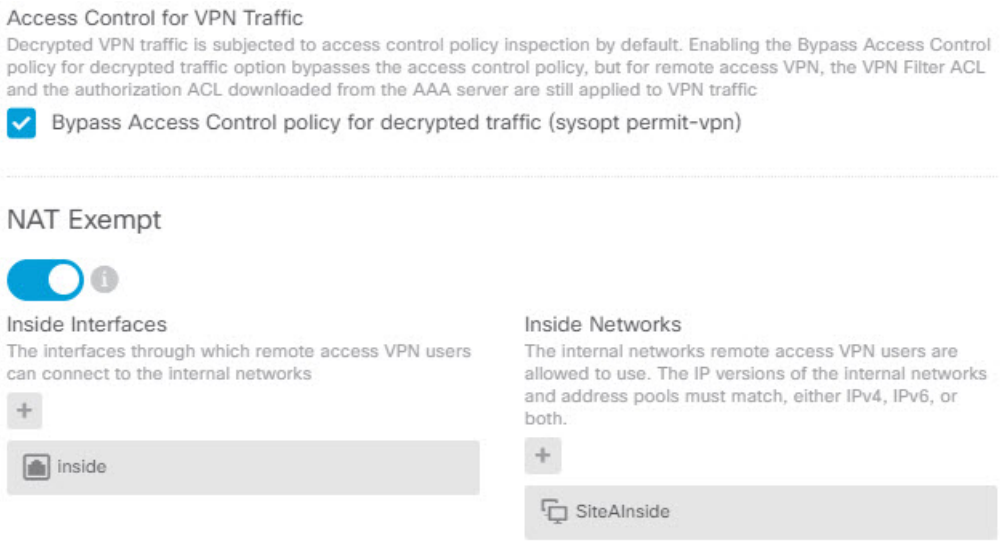
e) Cliquez sur **Next** (Suivant), puis sélectionnez une politique de groupe appropriée.

Vérifiez les renseignements récapitulatifs sur la politique que vous sélectionnez. Assurez-vous que les serveurs DNS sont configurés. Si ce n'est pas le cas, modifiez la politique maintenant et configurez le DNS.

f) Cliquez sur **Next** (Suivant), et dans les paramètres globaux, sélectionnez l'option **de contournement de la stratégie de contrôle d'accès pour le trafic déchiffré (sysopt permit-vpn)** et configurez les options **NAT Exempt** (Exemption NAT).

Pour **NAT Exempt** (Exemption NAT), vous devez configurer les options suivantes. Notez que si d'autres profils de connexion sont définis, vous devez ajouter aux paramètres existants, car la configuration s'applique à tous les profils de connexion.

- **Inside Interfaces** (Interfaces internes) : sélectionnez l'interface **inside**. Ce sont les interfaces des réseaux internes auxquels les utilisateurs distants accéderont. Les règles NAT sont créées pour ces interfaces.
- **Inside Networks** (Réseaux internes) : Sélectionnez l'objet réseau SiteAInside. Ce sont les objets réseau qui représentent les réseaux internes auxquels les utilisateurs distants accéderont.



g) Chargez les paquets client AnyConnect pour les plateformes que vous prenez en charge.

h) Cliquez sur **Next** (Suivant) et vérifiez les paramètres.

Tout d'abord, vérifiez que le résumé est correct.

Ensuite, cliquez sur **Instructions** pour voir ce que doivent faire les utilisateurs finaux pour installer initialement le logiciel client AnyConnect et vérifier qu'ils peuvent établir une connexion VPN. Cliquez sur **Copy** (Copier) pour copier ces instructions dans le presse-papiers et les coller dans un fichier texte ou un courriel.

i) Cliquez sur **Terminer**.

Étape 7 Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



Étape 8 Cliquez sur le bouton **Deploy Now** (Déployer maintenant) et attendez la fin du déploiement.

L'appareil du site A est maintenant prêt à accepter les connexions VPN d'accès à distance. Demandez à un utilisateur externe d'installer le client AnyConnect et d'établir une connexion VPN.

Vous pouvez confirmer la connexion en vous connectant à l'interface de ligne de commande du périphérique et en utilisant la commande **show vpn-sessiondb anyconnect** pour afficher les informations de session.

Comment contrôler l'accès VPN RA par groupe

Vous pouvez configurer des profils de connexion VPN d'accès à distance pour fournir un accès différentiel aux ressources internes en fonction de la politique de groupe. Par exemple, si vous souhaitez fournir un accès sans restriction aux employé(e)s, mais que les sous-traitants ne peuvent accéder qu'à un seul réseau interne et rien d'autre, vous pouvez utiliser les politiques de groupe pour définir différentes listes de contrôle d'accès afin de restreindre l'accès de manière appropriée.

L'exemple suivant montre comment configurer une connexion VPN d'accès à distance pour les sous-traitants qui doivent obtenir un accès au sous-réseau interne 192.168.2.0/24 uniquement. Pour les employés réguliers, vous pouvez utiliser la politique de groupe par défaut, qui n'a pas de filtre de trafic défini pour le VPN. Vous pouvez modifier la politique de groupe par défaut si vous souhaitez appliquer des restrictions à ces utilisateurs et appliquer une liste de contrôle d'accès bâtie comme décrit ci-dessous.

Avant de commencer

Cette procédure suppose que vous ayez déjà créé la source d'identité à utiliser pour les sous-traitants. Il peut s'agir d'une source différente de celle que vous utilisez pour les employé(e)s réguliers. Comme la source d'identité n'est pas strictement pertinente pour restreindre l'accès, nous l'avons omise dans cet exemple.

Cet exemple suppose également que l'interface « inside2 » est configurée pour héberger le sous-réseau 192.168.2.0/24, avec l'adresse IP 192.168.2.1 (toute autre adresse sur le sous-réseau est également acceptable).

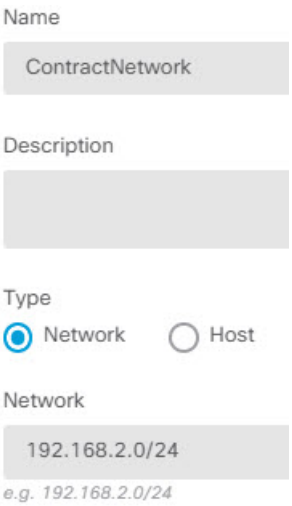
Procédure

Étape 1 Configurez la liste de contrôle d'accès (ACL) étendue pour restreindre le trafic VPN d'accès à distance.

Vous devez d'abord configurer l'objet réseau qui définit la cible 192.168.2.0/24, puis créer l'objet Smart CLI qui définit la liste d'accès. Comme la liste de contrôle d'accès comporte un refus implicite à la fin, vous n'avez qu'à autoriser l'accès au sous-réseau, et le trafic dirigé vers une adresse IP en dehors du sous-réseau sera refusé. Cet exemple s'applique uniquement à IPv4; vous pouvez également configurer des objets pour restreindre l'accès IPv6 à des sous-réseaux particuliers. Créez simplement l'objet réseau et ajoutez une commande ACE basée sur IPv6 à la même liste de contrôle d'accès.

a) Choisissez **Objects (Objets)** > **Networks (Réseaux)**, et créez l'objet requis.

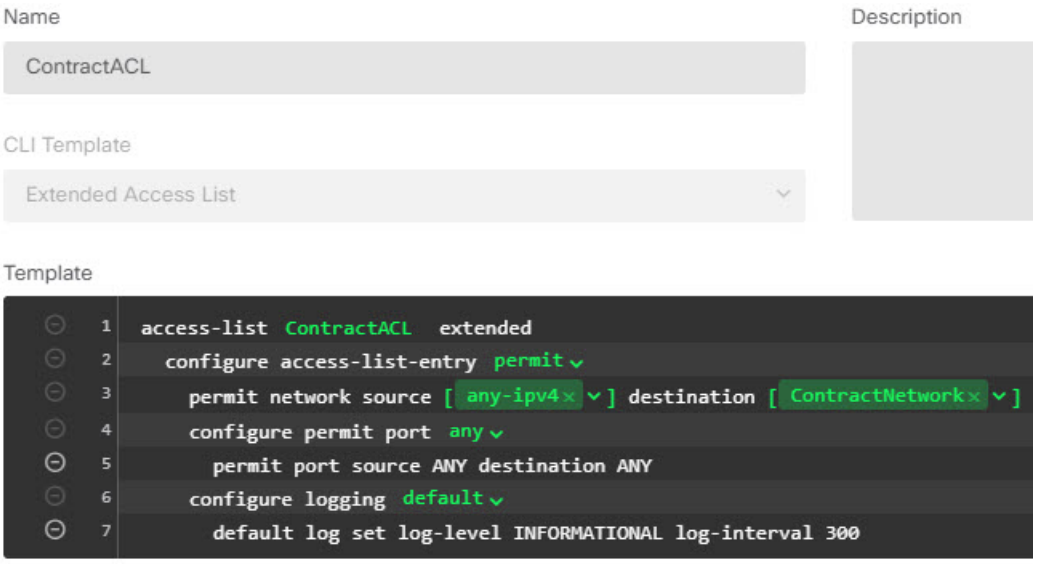
Par exemple, nommez l'objet ContractNetwork. Le corps de l'objet doit ressembler à ce qui suit :



b) Choisissez **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)** > **Smart CLI** > **Objects (Objets)**.
c) Cliquez + pour créer un nouvel objet.
d) Saisissez un nom pour la liste de contrôle d'accès. Par exemple, **ContractACL**.
e) Pour **CLI Template** (Modèle CLI), sélectionnez **Extended Access List** (Liste d'accès étendue).
f) Configurez les éléments suivants dans le **corps du modèle** :

- configurer l'action de liste d'accès = autoriser
- réseau-source = any-ipv4
- destination-network = objet ContractNetwork
- Configurer le port d'autorisation = tout
- Configurer la journalisation = par défaut

L'ACE doit ressembler à ce qui suit :



g) Cliquez sur **OK**.

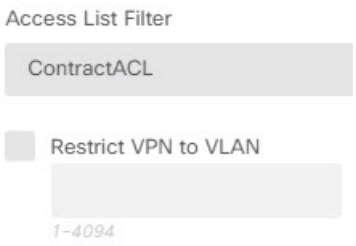
Cette liste de contrôle d'accès sera configurée lors du prochain déploiement de modifications. Vous n'avez pas besoin d'utiliser l'objet dans une autre politique pour forcer le déploiement.

Étape 2 Créez une politique de groupe qui utilise l'ACL.

Vous devez également configurer au minimum les serveurs DNS pour la politique de groupe. Configurez les options selon vos besoins. La procédure suivante se concentre sur le paramètre pertinent pour ce scénario.

a) Choisissez **Device (Périphérique)** > **RA VPN (VPN d'accès à distance)** > **Group Policies (Politiques de groupe)**.
b) Cliquez sur **+** pour créer une nouvelle politique de groupe.
c) Dans la page **General** (Général) , saisissez un nom pour la politique, par exemple **ContractGroup**.
d) Cliquez sur **Traffic Filters** (Filtres de trafic) dans la table des matières.
e) Pour **Access List Filter** (Filtre de liste d'accès), sélectionnez l'objet ContractACL.

Pour cet exemple, laissez l'option VLAN vide. Notez que vous pouvez également configurer un VLAN à des fins de filtrage et configurer une sous-interface pour le VLAN.



f) Cliquez sur **OK** pour enregistrer la politique de groupe.

Étape 3 Configurez le profil de connexion pour les sous-traitants.

a) Sur la page RA VPN (VPN d'accès à distance), cliquez sur **Connection Profiles** (Profils de connexion) dans la table des matières.
b) Cliquez sur **+** pour créer un nouveau profil de connexion.
c) Terminez l'étape 1 de l'assistant et cliquez sur **Next** (Suivant).

Saisissez un nom pour le profil, par exemple, Sous-traitants.

Configurez le reste des options comme d'habitude. Cela inclut la sélection de la source d'authentification appropriée pour les sous-traitants et la définition d'un ensemble d'adresses.

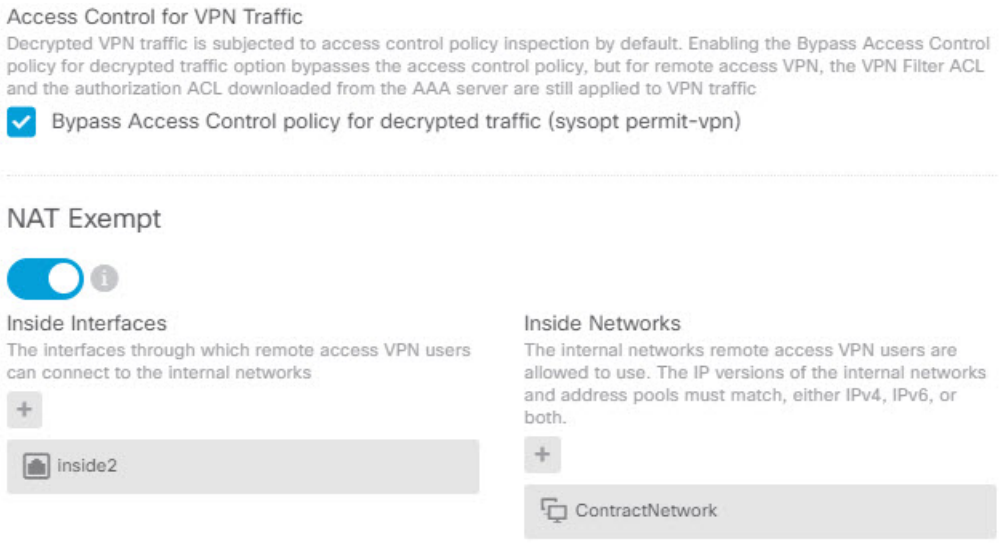
d) Sélectionnez la politique de groupe que vous avez configurée pour les sous-traitants, puis cliquez sur **Next** (Suivant).



e) Dans les paramètres globaux, sélectionnez l'option **Bypass Access Control policy for decrypted traffic** (Politique de contournement du contrôle d'accès pour le trafic déchiffré) (sysopt permit-vpn) et configurez les options **NAT Exempt** (Exemption NAT).

Pour **NAT Exempt** (Exemption NAT), vous devez configurer les options suivantes. Notez que si d'autres profils de connexion sont définis, vous devez ajouter aux paramètres existants, car la configuration s'applique à tous les profils de connexion.

- **Inside Interfaces** (Interfaces internes) : sélectionnez l'interface **inside2**. Ce sont les interfaces des réseaux internes auxquels les utilisateurs distants accéderont. Les règles NAT sont créées pour ces interfaces.
- **Inside Networks** (Réseaux internes) : sélectionnez l'objet réseau ContractNetwork. Ce sont les objets réseau qui représentent les réseaux internes auxquels les utilisateurs distants accéderont.



f) Chargez les paquets client AnyConnect pour les plateformes que vous prenez en charge.

g) Cliquez sur **Next** (Suivant) et vérifiez les paramètres.

Tout d'abord, vérifiez que le résumé est correct.

Ensuite, cliquez sur **Instructions** pour voir ce que doivent faire les utilisateurs finaux pour installer initialement le logiciel client AnyConnect et vérifier qu'ils peuvent établir une connexion VPN. Cliquez sur **Copy** (Copier) pour copier ces instructions dans le presse-papiers et les coller dans un fichier texte ou un courriel.

h) Cliquez sur **Terminer**.

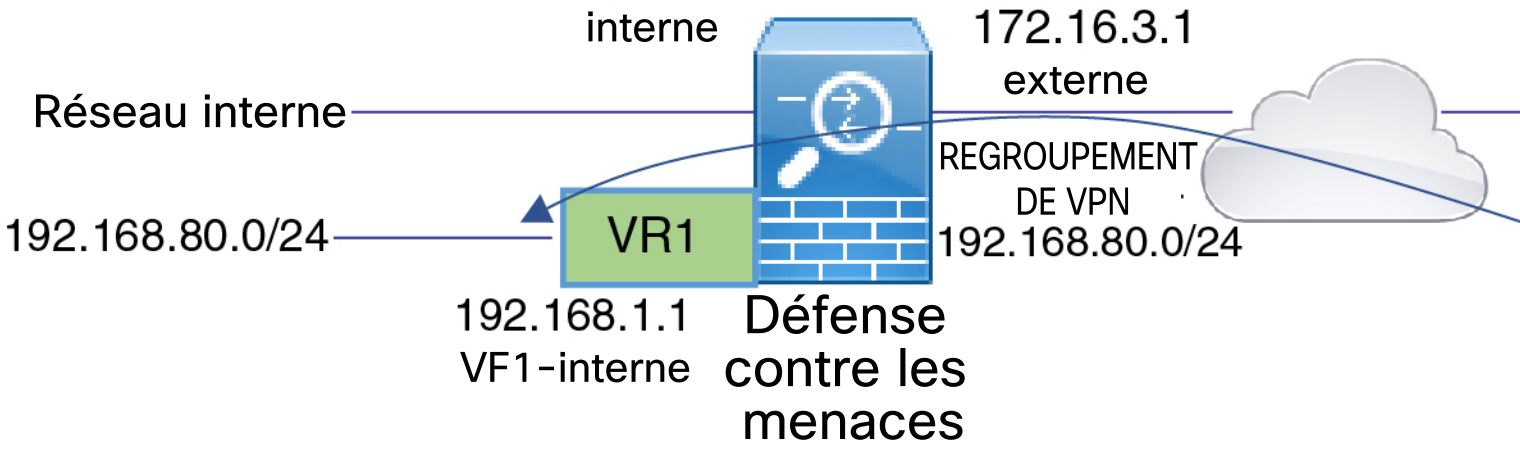
Comment autoriser l'accès au VPN d'accès à distance aux réseaux internes dans différents routeurs virtuels.

Si vous configurez plusieurs routeurs virtuels sur un périphérique, vous devez configurer le VPN d'accès distant dans le routeur virtuel global. Vous ne pouvez pas configurer le VPN d'accès distant sur une interface affectée à un routeur virtuel personnalisé.

Comme les tables de routage pour les routeurs virtuels sont distinctes, vous devez créer des routes statiques si vos utilisateurs de VPN d'accès distant doivent avoir accès à des réseaux qui font partie d'un autre routeur virtuel.

Considérez l'exemple suivant. Dans ce cas, l'utilisateur de VPN d'accès distant se connecte à l'interface externe à l'adresse 172.16.3.1 et reçoit une adresse IP dans le pool de 192.168.80.0/24. Cet utilisateur peut maintenant accéder au réseau interne qui est attaché au routeur virtuel global. Cependant, l'utilisateur ne peut

pas atteindre le réseau 192.168.1.0/24 qui fait partie du routeur virtuel VR1. Pour permettre le flux de trafic entre le réseau VR1 et l'utilisateur VPN d'accès distant, vous devez configurer des routes statiques dans les deux sens.



Avant de commencer

Cet exemple suppose que vous ayez déjà configuré de VPN d'accès à distance, défini les routeurs virtuels et configuré et affecté les interfaces aux routeurs virtuels appropriés.

Procédure

Étape 1 Configurez la fuite de route du routeur virtuel global vers VR1.

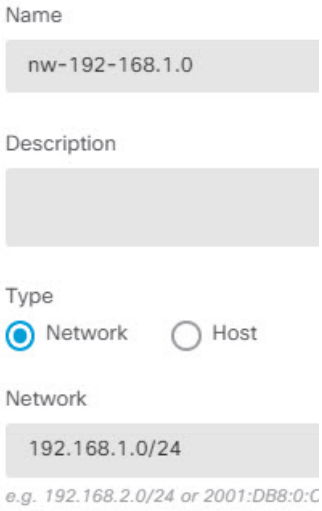
Cette route permet aux adresses IP client AnyConnect attribuées dans l'ensemble d'adresses du VPN d'accéder au réseau 192.168.1.0/24 du routeur virtuel VR1.

a) Choisissez **Device (Périphérique)** > **Routing (Routage)** > **View Configuration (Afficher la configuration)**.

b) Cliquez sur l'icône d'affichage ( ) du routeur virtuel global.

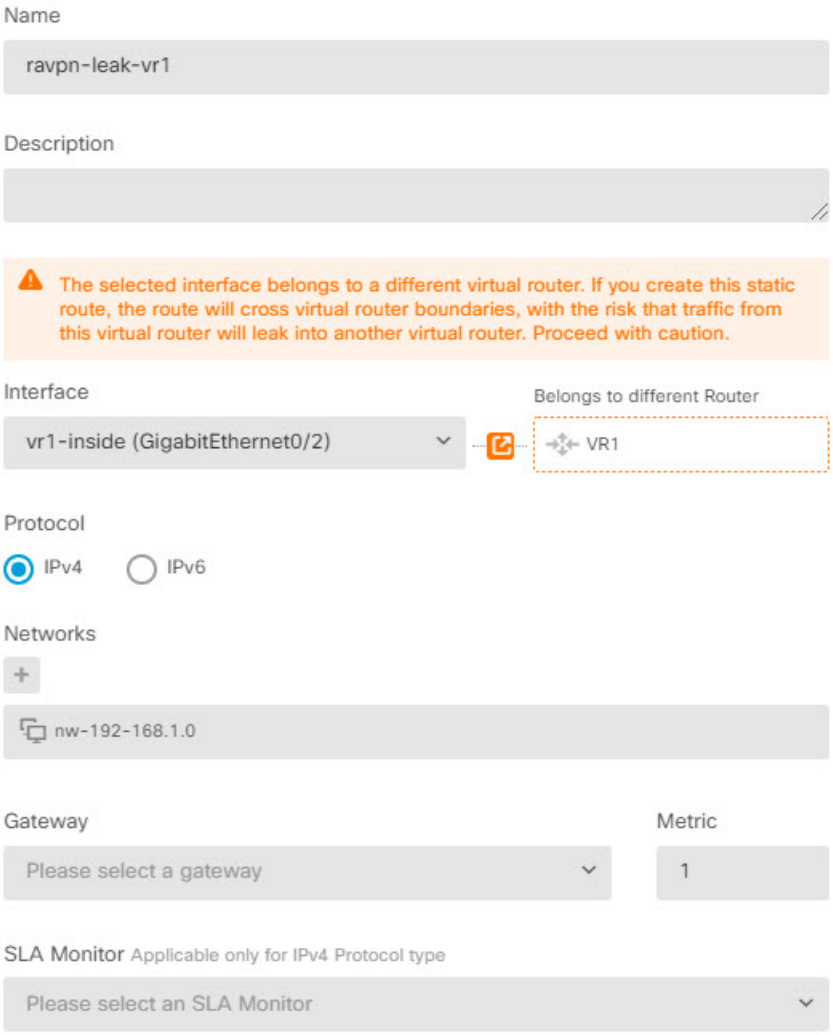
c) Dans l'onglet **Static Routing** (Routage statique) du routeur virtuel global, cliquez sur + et configurez la route :

- **Nom** : n'importe quel nom suffit, tel que **ravpn-leak-vr1**.
- **Interface** : sélectionnez **vr1-inside**.
- **Protocole** : sélectionnez **IPv4**.
- **Réseaux** : sélectionnez un objet qui définit le réseau 192.168.1.0/24. Cliquez sur **Create New Network** (Créer un nouveau réseau) pour créer l'objet maintenant, si nécessaire.



- **Gateway** (passerelle) : laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



d) Cliquez sur **OK**.

Étape 2 Configurez la fuite de route de VR1 vers le routeur virtuel global :

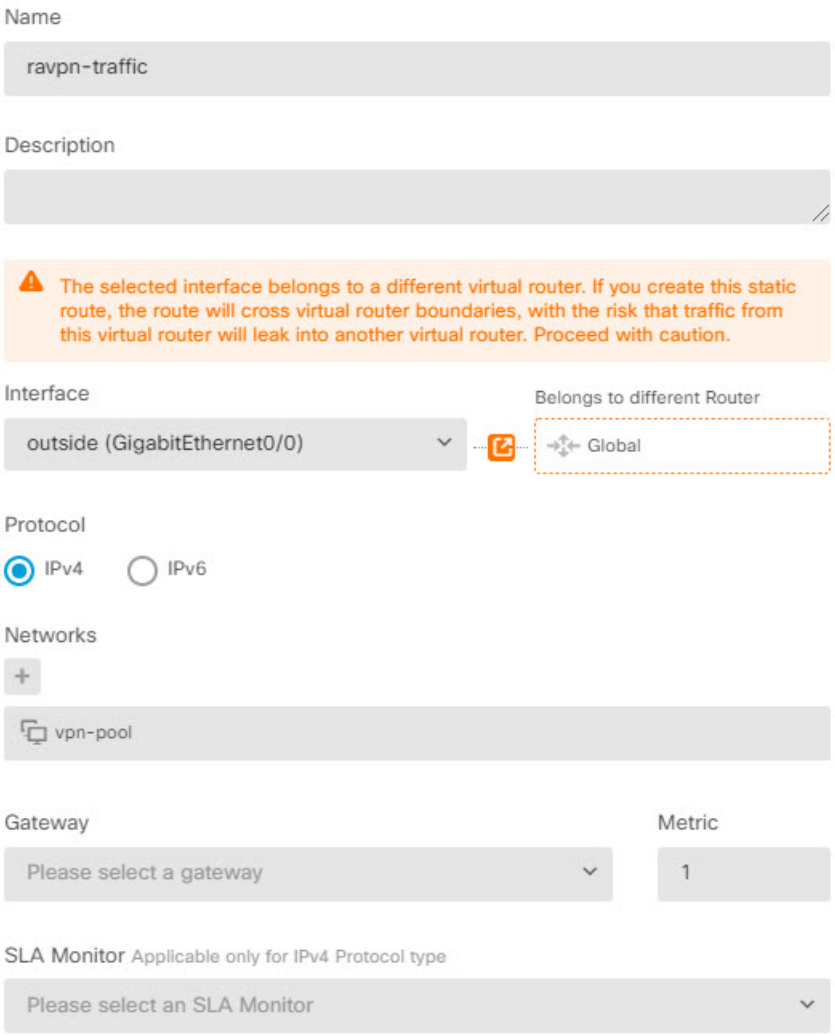
Cette route permet aux points terminaux sur le réseau 192.168.1.0/24 d'établir des connexions avec les client AnyConnect adresses IP attribuées dans l'ensemble d'adresses du VPN.

a) Choisissez **VR1** dans la liste déroulante des routeurs virtuels pour passer à la configuration VR1.

b) Dans l'onglet **Static Routing** (Routage statique) du routeur virtuel VR1, cliquez sur + et configurezla route :

- **Nom** : n'importe quel nom suffit, tel que **ravpn-trafic**.
- **Interface** : sélectionnez **outside**.
- **Protocole** : sélectionnez **IPv4**.
- **Réseaux** : sélectionnez l'objet que vous avez créé pour le regroupement VPN, par exemple, **vpn-pool**.
- **Gateway** (passerelle) : laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



c) Cliquez sur **OK**.

Prochaine étape

Si l'ensemble d'adresses du VPN d'accès à distance et les adresses IP du routeur virtuel défini par l'utilisateur se chevauchent, vous devez également utiliser des règles NAT statiques sur les adresses IP pour permettre un routage approprié. Cependant, il est beaucoup plus facile de modifier simplement votre ensemble d'adresses VPN d'accès à distance afin d'éviter les chevauchements.

Comment personnaliser l'icône et le logo client AnyConnect

Vous pouvez personnaliser l'icône et le logo de l'application client AnyConnect sur les machines clients Windows et Linux. Les noms des icônes sont prédéfinis et il existe des limites précises au type de fichier et à la taille des images que vous téléversez.

Bien que vous puissiez utiliser n'importe quel nom de fichier si vous déployez votre propre exécutable pour personnaliser l'interface graphique, cet exemple suppose que vous échangez simplement des icônes et des logos sans déployer une structure entièrement personnalisée.

Il existe un certain nombre d'images que vous pouvez remplacer, et leurs noms de fichiers varient selon la plateforme. Pour obtenir des renseignements complets sur les options de personnalisation, les noms de fichiers, les types et les tailles, consultez le chapitre sur la personnalisation et la localisation du client AnyConnect et de l'installateur dans le *Guide de l'administrateur du client Secure Client AnyConnect Secure Mobility Client*. Par exemple, le chapitre du client 4.8 est disponible à l'adresse :

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html

Avant de commencer

Aux fins de cet exemple, nous remplacerons les images suivantes pour les clients Windows. Notez que si votre image est de taille différente de la taille maximale, le système la redimensionnera automatiquement au maximum et étendra automatiquement l'image au besoin.

- app_logo.png

  Cette image de logo d'application est l'icône de l'application. Elle peut avoir une taille maximale de 128 x 128 pixels.

- company_logo.png

  Cette image de logo d'entreprise apparaît dans le coin supérieur gauche des commandes déroulantes du tiroir et des boîtes de dialogue Advanced (Avancé). La taille maximale est de 97 x 58 pixels.

- company_logo_alt.png

  L'autre image de logo d'entreprise apparaît dans le coin inférieur droit de la boîte de dialogue À propos de. La taille maximale est de 97 x 58 pixels.

Pour téléverser ces fichiers, vous devez les placer sur un serveur auquel l'appareil Firewall Threat Defense peut accéder. Vous pouvez utiliser un serveur TFTP, FTP, HTTP, HTTPS ou SCP. Les URL pour obtenir des images de ces fichiers peuvent inclure des chemins d'accès et un nom d'utilisateur/mot de passe, comme requis par la configuration de votre serveur. Cet exemple utilisera TFTP.

Procédure

Étape 1 Chargez les fichiers image sur chaque périphérique Firewall Threat Defense agissant comme tête de réseau VPN d'accès à distance et devant utiliser les icônes et logos personnalisés.

a) Connectez-vous à l'interface de ligne de commande (CLI) de l'appareil à l'aide d'un client SSH.

b) Dans l'interface de ligne de commande, saisissez la commande **system support diagnostic-cli** pour passer en mode de diagnostic de l'interface de ligne de commande.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv1>
```

Remarque

Lisez le message ! Vous devez appuyer sur **Ctrl + a, puis sur d**, pour sortir de l'interface de commande en ligne de diagnostic et revenir en mode d'interface de commande en ligne normal.Firewall Threat Defense

c) Notez l'invite de commande. La CLI normale utilise uniquement les >, tandis que le mode EXEC de l'interface de diagnostic en ligne de diagnostic utilise le nom d'hôte plus >. Dans cet exemple, ftdv1>. Vous devez passer en mode d'exécution privilégié, qui utilise # comme caractère de fin, par exemple, ftdv1#. Si votre invite contient déjà le numéro, ignorez cette étape. Sinon, saisissez la commande enable, puis appuyez simplement sur Enter (Entrée) à l'invite de mot de passe, et ce, sans saisir de mot de passe.

```
ftdv1> enable
Password:
ftdv1#
```

d) Utilisez la commande **copy** pour copier chaque fichier du serveur d'hébergement dans le disk0 (disque0) du périphérique.Firewall Threat Defense Vous pouvez les placer dans un sous-répertoire, tel que disk0:/anyconnect-images/. Vous pouvez créer un nouveau dossier en utilisant la commande **mkdir**.

Par exemple, si l'adresse IP du serveur TFTP est 10.7.0.80 et que vous souhaitez créer un nouveau répertoire, les commandes seront semblables aux suivantes. Notez que les réponses à la commande **copy** sont omises après le premier exemple.

```
ftdv1# mkdir disk0:anyconnect-images

Create directory filename [anyconnect-images]? yes

Created dir disk0:/anyconnect-images

ftdv1# copy /noconfirm tftp://10.7.0.80/app_logo.png
disk0:/anyconnect-images/app_logo.png

Accessing tftp://10.7.0.80/app_logo.png...!!!!!!
Writing file disk0:/anyconnect-images/app_logo.png...
!!!!!!
12288 bytes copied in 1.000 secs (12288 bytes/sec)

ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo.png
disk0:/anyconnect-images/company_logo.png
ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo_alt.png
disk0:/anyconnect-images/company_logo_alt.png
```

Étape 2 Utilisez la commande **import webvpn** dans l'interface de ligne de commande de diagnostic, pour demander au périphérique de télécharger ces images lors de son installation sur les machines clientes.client AnyConnect

import webvpn AnyConnect-customization type resource platform win name *filename* **disk0:**/*directoryname/filename*

Cette commande concerne Windows. Pour Linux, remplacez le mot-clé **win** par **linux** ou **linux-64**, selon le cas pour vos clients.

Par exemple, pour importer les fichiers téléchargés à l'étape précédente, et en supposant que nous sommes toujours dans l'interface de ligne de commande de diagnostic :

```
ftdv1# import webvpn AnyConnect-customization type resource platform win
name app_logo.png disk0:/anyconnect-images/app_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
```

```
name company_logo.png disk0:/anyconnect-images/company_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png disk0:/anyconnect-images/company_logo_alt.png
```

Étape 3 Vérifiez la configuration.

- Pour vérifier les fichiers importés, utilisez la commande **show import webvpn AnyConnect-customization** en mode d'exécution privilégié de la CLI de diagnostic.
- Pour vérifier que les images ont été téléchargées sur un client, elles doivent apparaître lorsque l'utilisateur exécute le client. Vous pouvez également vérifier le dossier suivant sur les clients Windows, où %PROGRAMFILES% se résout généralement en c:\Program Files.

  %PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res

Prochaine étape

Si vous souhaitez revenir aux images par défaut, utilisez la commande **revert webvpn** (en mode d'exécution privilégié de la CLI de diagnostic) pour chaque image que vous avez personnalisée. La commande est :

revert webvpn AnyConnect-customization type resource platform win name *nom de fichier*

Comme pour **import webvpn**, remplacez **win** par **linux** ou **linux-64** si vous avez personnalisé ces plateformes clientes, et exécutez la commande séparément pour chaque nom de fichier d'image que vous avez importé. Par exemple :

```
ftdv1# revert webvpn AnyConnect-customization type resource platform win
name app_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png
```



PARTIE VII

Administration système

- Paramètres système, à la page 785
- Gestion du système, à la page 819



CHAPITRE 26

Paramètres système

Les rubriques suivantes expliquent comment configurer les différents paramètres système qui sont regroupés sur la page Paramètres système. Les paramètres couvrent le fonctionnement global du système.

- Configurer l'accès de gestion, à la page 785
- Configurer les paramètres de journalisation du système, à la page 789
- Configuration du serveur DHCP, à la page 795
- Configurer le DNS, à la page 797
- Configuration de l'interface de gestion, à la page 802
- Configurer le nom d'hôte du périphérique., à la page 804
- Protocole de temps réseau (NTP), à la page 804
- Configuration du protocole Precision Time Protocol (PTP) (ISA 3000), à la page 805
- Configuration du serveur mandataire HTTP pour les connexions de gestion, à la page 808
- Configuration de Cisco Cloud Services, à la page 809
- Activation ou désactivation de l'analyse Web, à la page 814
- Configuration des préférences de filtrage Cloud , à la page 814
- Configuration des paramètres de chiffrement TLS/SSL, à la page 815

Configurer l'accès de gestion

L'accès de gestion fait référence à la capacité de se connecter au périphérique Firepower Threat Defense à des fins de configuration et de surveillance. Vous pouvez configurer les éléments suivants :

- AAA pour identifier la source d'identité à utiliser pour authentifier l'accès des utilisateurs. Vous pouvez utiliser la base de données d'utilisateurs locale ou un serveur AAA externe. Pour plus d'informations sur la gestion des utilisateurs administratifs, consultez Gestion du Gestionnaire de périphériques de pare-feu et accès des utilisateurs Firewall Threat Defense, à la page 843.
- Contrôle d'accès à l'interface de gestion et aux interfaces de données. Il existe des listes d'accès distinctes pour ces interfaces. Vous pouvez décider quelles adresses IP sont autorisées pour HTTPS (utilisé pour le Gestionnaire de périphériques de pare-feu) et SSH (utilisé pour l'interface de ligne de commande). Consultez Configuration de la liste d'accès de gestion, à la page 786.
- Le certificat du serveur Web de gestion, que les utilisateurs doivent accepter pour se connecter à Gestionnaire de périphériques de pare-feu. En chargeant un certificat auquel vos navigateurs Web font déjà confiance, vous évitez de demander aux utilisateurs d'approuver un certificat inconnu. Consultez Configuration du certificat du serveur Web Firewall Threat Defense, à la page 788.

Configuration de la liste d'accès de gestion

Par défaut, vous pouvez atteindre les interfaces Web ou de l'interface de ligne de commande FDM de l'appareil sur l'adresse de gestion à partir de n'importe quelle adresse IP. L'accès au système est protégé uniquement par un nom d'utilisateur et un mot de passe. Cependant, vous pouvez configurer une liste d'accès pour autoriser les connexions à partir d'adresses IP ou de sous-réseaux spécifiques uniquement pour fournir un autre niveau de protection.

Vous pouvez également ouvrir des interfaces de données pour permettre les connexions Gestionnaire de périphériques de pare-feu ou de SSH à l'interface de ligne de commande. Vous pouvez ensuite gérer l'appareil sans utiliser l'adresse de gestion. Par exemple, vous pouvez autoriser l'accès de gestion à l'interface externe, afin de pouvoir configurer le périphérique à distance. Le nom d'utilisateur et le mot de passe offre une protection contre les connexions indésirables. Par défaut, l'accès de gestion HTTPS aux interfaces de données est activé sur l'interface interne, mais désactivé sur l'interface externe. Pour le Firepower 1010 qui possède un groupe de ponts « intérieur » par défaut, cela signifie que vous pouvez effectuer les connexions de Gestionnaire de périphériques de pare-feu au moyen de n'importe quelle interface de données au sein du groupe de ponts vers l'adresse IP du groupe de pont (par défaut 192.168.95.1). Vous pouvez ouvrir une connexion de gestion uniquement sur l'interface au moyen de laquelle vous accédez à l'appareil.

⚠

Mise en garde Si vous limitez l'accès à des adresses spécifiques, vous pouvez facilement vous exclure du système. Si vous supprimez l'accès pour l'adresse IP que vous utilisez actuellement et qu'il n'y a aucune entrée pour n'importe quelle adresse, vous perdrez l'accès au système lorsque vous déploierez la politique. Soyez très prudent si vous décidez de configurer la liste d'accès.

Avant de commencer

Vous ne pouvez pas configurer à la fois l'accès (accès HTTPS) FDM et le VPN SSL d'accès à distance AnyConnect sur la même interface pour le même port TCP. Par exemple, si vous configurez le VPN SSL d'accès distant sur l'interface externe, vous ne pouvez pas ouvrir aussi l'interface externe pour les connexions HTTPS sur le port 443. Si vous configurez les deux fonctionnalités sur la même interface, veillez à modifier le port HTTPS d'au moins l'un de ces services pour éviter un conflit.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur le lien **System Settings** > **Management Access**.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **Management Access (accès de gestion)** dans la table des matières.

Vous pouvez également configurer AAA sur cette page pour autoriser l'accès de la gestion aux utilisateurs définis dans un serveur AAA externe. Pour de plus amples renseignements, consultez la section Gestion du Gestionnaire de périphériques de pare-feu et accès des utilisateurs Firewall Threat Defense, à la page 843.

Étape 2 Pour créer des règles pour l'adresse de gestion :

a) Sélectionnez l'onglet **Management Interface** (interface de gestion).

La liste des règles définit quelles adresses sont autorisées à accéder au port indiqué : 443 pour le Gestionnaire de périphériques de pare-feu (l'interface Web HTTPS), 22 pour l'interface de ligne de commande SSH.

Les règles ne composent pas une liste ordonnée. Si une adresse IP correspond à une règle du port demandé, l'utilisateur est autorisé à tenter de se connecter au périphérique.

Remarque

Pour supprimer une règle, cliquez sur l'icône de la corbeille ( ) de la règle. Si vous supprimez toutes les règles d'un protocole, personne ne pourra accéder au périphérique sur cette interface à l'aide du protocole.

b) Cliquez sur + et complétez les options suivantes :

- **Protocol** (protocole) : Précisez si la règle est pour HTTPS (port 443) ou SSH (port 22).
- **IP Address** (adresse IP) : Sélectionnez l'objet réseau qui définit le réseau ou l'hôte IPv4 ou IPv6 qui devrait pouvoir accéder au système. Pour spécifier la sélection de « toute » adresse, sélectionnez **any-ipv4** (0.0.0.0/0) et **any-ipv6** (::/0).

c) Cliquez sur **OK**.

Étape 3 Pour créer des règles pour les interfaces de données :

a) Sélectionnez l'onglet **Data Interfaces** (interfaces de données).

La liste des règles définit quelles adresses sont autorisées à accéder au port indiqué sur l'interface : 443 pour le Gestionnaire de périphériques de pare-feu (l'interface Web HTTPS), 22 pour l'interface de ligne de commande SSH.

Les règles ne composent pas une liste ordonnée. Si une adresse IP correspond à une règle du port demandé, l'utilisateur est autorisé à tenter de se connecter au périphérique.

Remarque

Pour supprimer une règle, cliquez sur l'icône de la corbeille ( ) de la règle. Si vous supprimez toutes les règles d'un protocole, personne ne pourra accéder au périphérique sur cette interface à l'aide du protocole.

b) Cliquez sur + et complétez les options suivantes :

- **Interface** : Sélectionnez l'interface sur laquelle vous souhaitez autoriser l'accès de gestion.
- **Protocols** (protocoles) : Précisez si la règle est pour HTTPS (port 443), pour SSH (port 22) ou les deux. Vous ne pouvez pas configurer les règles HTTPS pour l'interface externe si elle est utilisée dans un profil de connexion VPN d'accès distant.
- **Allowed Networks (réseaux permis)** : Sélectionnez les objets réseau qui définissent le réseau ou l'hôte IPv4 ou IPv6 qui devrait pouvoir accéder au système. Pour spécifier la sélection de « toute » adresse, sélectionnez **any-ipv4** (0.0.0.0/0) et **any-ipv6** (::/0).

c) (Facultatif) Si vous souhaitez modifier le numéro de port de données HTTPS, cliquez sur le numéro et entrez un nouveau port. Consultez Configuration du port HTTPS pour l'accès de gestion sur les interfaces de données, à la page 788

d) Cliquez sur **OK**.

Configuration du port HTTPS pour l'accès de gestion sur les interfaces de données

Par défaut, l'accès à l'appareil à des fins de gestion, que ce soit pour le Gestionnaire de périphériques de pare-feu ou l'API Firewall Threat Defense, se fait au moyen du port TCP/443. Vous pouvez modifier le port d'accès de gestion pour les interfaces de données.

Si vous modifiez le port, les utilisateurs doivent inclure le port personnalisé sur l'URL pour accéder au système. Par exemple, si l'interface de données est ftd.exemple.com et que vous changez le port pour 4443, les utilisateurs doivent modifier l'URL en https://ftd.exemple.com :4443.

Toutes les interfaces de données utiliseront le même port. Vous ne pouvez pas configurer différents ports par interface.

Remarque Vous ne pouvez pas modifier le port d'accès de gestion pour l'interface de gestion. L'interface de gestion utilise toujours le port 443.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis cliquez sur le lien**System Settings** > **Management Access**.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **Management Access List** (liste d'accès de gestion) dans la table des matières.

Étape 2 Cliquez sur l'onglet **Data Interfaces** (interfaces de données).

Étape 3 Cliquez sur le numéro de port de données HTTPS (**HTTPS Data Port**).

Étape 4 Dans la boîte de dialogue Data Interfaces Setting, remplacez le port de données HTTPS (**HTTPS Data Port**) par celui que vous souhaitez utiliser.

Vous ne pouvez pas indiquer les numéros suivants :

- Le numéro 22, car il est utilisé pour les connexions SSH.
- Le port utilisé pour le VPN d'accès distant, si vous l'avez configuré pour n'importe quelle interface que vous autorisez également pour l'accès de gestion. Le VPN d'accès à distance utilise le port 443 par défaut, mais vous pouvez configurer un port personnalisé pour ce port.
- Le port utilisé pour l'authentification active dans la politique d'identité, qui est 885 par défaut.

Étape 5 Cliquez sur **OK**.

Configuration du certificat du serveur Web Firewall Threat Defense

Lorsque vous vous connectez à l'interface Web, le système utilise un certificat numérique pour sécuriser les communications via HTTPS. Le certificat par défaut n'est pas sécurisé par votre navigateur, donc un avertissement d'autorité non fiable s'affiche et vous demande si vous souhaitez faire confiance au certificat.

Bien que les utilisateurs puissent enregistrer le certificat dans le magasin de certificats racine de confiance, vous pouvez plutôt charger un nouveau certificat que les navigateurs sont déjà configurés pour faire confiance.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis cliquez sur le lien**System Settings** > **Management Access**.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **Management Access List** (liste d'accès de gestion) dans la table des matières.

Étape 2 Cliquez sur l'onglet **Management Web Server** (Serveur Web de gestion).

Étape 3 Dans **Web Server Certificate** (Certificat du serveur Web), sélectionnez le certificat interne à utiliser pour sécuriser les connexions HTTPS avec le Gestionnaire de périphériques de pare-feu.

Si vous n'avez pas chargé ou créé le certificat, cliquez sur le lien **Create New Internal Certificate** (créer un nouveau certificat interne) au bas de la liste et créez-le maintenant.

La valeur par défaut est l'objet prédéfini DefaultWebserverCertificate.

Étape 4 Si le certificat n'est pas autosigné, ajoutez tous les certificats intermédiaires et les certificats racine de la chaîne de confiance complète à la liste **Trusted Chain** (chaîne de confiance).

Vous pouvez ajouter jusqu'à 10 certificats dans la chaîne. Cliquez sur le signe **plus (+)** pour ajouter chaque certificat intermédiaire, et finalement, le certificat racine. Lorsque vous cliquez sur **Save** (Enregistrer) (puis **Proceed** (Continuer) dans la boîte de dialogue vous avertissant que le serveur Web redémarrera, si un certificat est manquant, vous obtenez un message d'erreur avec le nom commun du certificat suivant de la chaîne qui est manquant. Vous obtiendrez également une erreur si vous ajoutez un certificat qui ne fait pas partie de la chaîne. Examinez ces messages avec soin pour identifier le certificat que vous devez ajouter ou supprimer.

Vous pouvez charger les certificats à partir d'ici en cliquant sur **Create New Trusted CA Certificate** (Créer un nouveau certificat CA de confiance) après avoir cliqué sur **+**.

Étape 5 Cliquez sur **Save** (enregistrer).

La modification est appliquée immédiatement et le système redémarre le serveur Web. Vous n'avez pas besoin de déployer la configuration.

Attendez quelques minutes que le serveur Web redémarre, puis actualisez votre navigateur.

Configurer les paramètres de journalisation du système

Vous pouvez activer la journalisation du système (syslog) pour les périphériques Firewall Threat Defense. Les informations de journalisation peuvent vous aider à cerner et isoler les problèmes de configuration du réseau ou des périphériques. Vous pouvez activer syslog pour la journalisation des diagnostics ainsi que pour la journalisation liée aux connexions, y compris le contrôle d'accès, la prévention des intrusions et la journalisation des fichiers et des programmes malveillants.

La journalisation des diagnostics fournit des messages syslog pour les événements liés à l'intégrité des périphériques et du système, et à la configuration du réseau, qui ne sont pas liés aux connexions. Vous configurez la journalisation des connexions dans les règles de contrôle d'accès individuelles.

La journalisation des diagnostics génère des messages pour les fonctionnalités exécutées sur le plan de données, c'est-à-dire les fonctionnalités qui sont définies dans la configuration de l'interface de ligne de commande que vous pouvez afficher à l'aide de la commande **show running-config**. Cela inclut des fonctionnalités telles que le routage, le VPN, les interfaces de données, le serveur DHCP, la NAT, etc.

Pour en savoir plus sur ces messages, consultez la documentation *Messages syslog de Cisco Threat Defense* à l'adresse https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html.

Les rubriques suivantes expliquent comment configurer la journalisation des messages de diagnostic et de fichiers/programmes malveillants vers différents emplacements de sortie.

Niveaux de gravité

Le tableau suivant répertorie les niveaux de gravité des messages du journal système.

Tableau 17 : Niveaux de gravité des messages Syslog

Numéro de niveau	Niveau de gravité	Description
0	**urgences**	Système inutilisable.
1	**alerte**	Action immédiate requise.
2	**critique**	Conditions critiques.
3	**erreur**	Conditions d'erreur.
4	**avertissement**	Conditions de mise en garde.
5	**notification**	Condition normale, mais pouvant être grave
6	**renseignements**	Messages informatifs seulement.
7	**débogage**	Messages de débogage uniquement Ne journalisez à ce niveau que temporairement, lors du débogage des problèmes. Ce niveau de journalisation peut générer tant de messages que les performances du système peuvent en être affectées.

Remarque ASA et FTD ne génèrent pas de messages syslog avec un niveau de gravité de zéro (urgences).

Configurer la journalisation vers un serveur Syslog distant

Vous pouvez configurer le système pour envoyer des messages de journal système à un serveur de journaux système externe. Il s'agit de la meilleure option pour la journalisation du système. En utilisant un serveur externe, vous pouvez disposer de plus d'espace pour contenir les messages et utiliser les installations du serveur pour afficher, analyser et archiver les messages.

En outre, si vous appliquez des politiques de fichiers au trafic dans les règles de contrôle d'accès, pour contrôler l'accès aux fichiers ou les programmes malveillants, ou les deux, vous pouvez configurer le système pour

envoyer des messages d'événement de fichier à un serveur syslog externe. Si vous ne configurez pas de serveur syslog, les événements sont disponibles uniquement dans Event Viewer (Visionneuse d'événements) Gestionnaire de périphériques de pare-feu.

La procédure suivante explique comment activer syslog pour la journalisation des diagnostics (données) et la journalisation des fichiers et des programmes malveillants. Vous pouvez également configurer la journalisation externe pour les éléments suivants :

- Les événements de connexion, en sélectionnant le serveur syslog dans les règles de contrôle d'accès individuelles, les règles de déchiffrement SSL ou les paramètres de politique Security Intelligence.
- Les incidents d'intrusion, en sélectionnant le serveur syslog dans les paramètres de la politique de prévention des intrusions.

Avant de commencer

Le paramètre syslog pour les événements liés aux fichiers ou aux programmes malveillants n'est pertinent que si vous appliquez des politiques de fichiers ou de programmes malveillants, lesquelles nécessitent les licences Threat et .

En outre, vous devez vous assurer que l'option **File Events (Événements de fichiers)** > **Log Files (Fichiers journaux)** est sélectionnée dans les règles de contrôle d'accès qui appliquent ces politiques. Sinon, aucun événement n'est généré, que ce soit pour syslog ou pour Event Viewer (Visionneuse d'événements).

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis cliquez sur le lien **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation)**.

Si vous êtes déjà dans la page des paramètres système, cliquez simplement sur **Logging Settings** (Paramètres de journalisation) dans la table des matières.

Étape 2 Sous **Remote Server** (Serveur distant), placez le curseur **Data Logging** (Journalisation des données) sur **On** (Activé) pour activer la journalisation des messages de diagnostic générés par le plan de données sur un serveur syslog externe. Configurez les options suivantes :

- **Syslog Server** (Serveur Syslog) : cliquez sur le signe **(+)** et sélectionnez un ou plusieurs objets de serveur syslog, puis cliquez sur **OK**. Si les objets n'existent pas, cliquez sur le lien **Add Syslog Server** (Ajouter un serveur Syslog) et créez-les maintenant. Pour en savoir plus, consultez Configuration des serveurs Syslog, à la page 154.
- **Niveau de gravité pour le filtrage des journaux système de châssis FXOS** : pour certains modèles de périphériques qui utilisent FXOS, le niveau de gravité des messages syslog générés par la plateforme FXOS de base. Cette option s'affiche uniquement si elle est pertinente pour votre périphérique. Sélectionnez le niveau de gravité. Les messages de ce niveau ou d'un niveau supérieur sont envoyés au serveur syslog.
- **Message Filtering** (Filtrage des messages) : sélectionnez l'une des options suivantes pour contrôler les messages générés pour le système d'exploitation Firewall Threat Defense.
  - **Severity Level for Filtering All Events** (Niveau de gravité pour le filtrage de tous les événements) : sélectionnez le niveau de gravité. Les messages de ce niveau ou d'un niveau supérieur sont envoyés au serveur syslog.

- **Custom Logging Filter** (Filtre de journalisation personnalisé) : si vous souhaitez effectuer un filtrage supplémentaire des messages, afin de n'obtenir que les messages qui vous intéressent, sélectionnez le filtre de liste d'événements qui définit les messages que vous souhaitez générer. Si le filtre n'existe pas déjà, cliquez sur **Create New Event List Filter** (Créer un nouveau filtre de liste d'événements) et créez-le maintenant. Pour en savoir plus, consultez Configurer Event List Filters (Filtres de liste d'événements), à la page 793.

Étape 3 Placez le curseur **File/Malware** (Fichiers/Programmes malveillants) sur **On (Activé)** pour activer la journalisation vers un serveur syslog externe pour les événements liés aux fichiers et aux programmes malveillants. Configurez ensuite les options de journalisation des fichiers et des programmes malveillants :

- **Syslog Server** (Serveur Syslog) : sélectionnez l'objet serveur syslog. Si l'objet n'existe pas, cliquez sur le lien **Add Syslog Server** (Ajouter un serveur Syslog) et créez-le maintenant.
- **Log at Severity Level** (Journaliser au niveau de gravité) : sélectionnez un niveau de gravité à attribuer aux événements liés aux fichiers/aux programmes malveillants. Comme tous les événements liés aux fichiers/aux programmes malveillants sont générés au même niveau de gravité, aucun filtrage n'est effectué ; vous verrez tous les événements, peu importe le niveau choisi. Il s'agit du niveau affiché dans le champ de gravité du message (c'est-à-dire le x dans FTD-x-<message_ID>). Les événements de fichiers utilisent l'ID de message 430004, les événements de programmes malveillants sont 430005.

Étape 4 Cliquez sur **Save** (Enregistrer).

Configuration de la journalisation dans le tampon interne

Vous pouvez configurer le système pour enregistrer les messages de journal système dans un tampon de journalisation interne. Utilisez la commande **show logging** dans l'interface de ligne de commande ou la console d'interface de ligne de commande pour afficher le contenu de la mémoire tampon.

Les nouveaux messages s'ajoutent à la fin du tampon. Lorsque la mémoire tampon est remplie, le système l'efface et continue d'y ajouter des messages. Lorsque la mémoire tampon de journal est pleine, le système supprime le message le plus ancien pour faire de la place dans la mémoire tampon pour les nouveaux messages.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis cliquez sur le lien **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation)**.

Si vous êtes déjà dans la page des paramètres système, cliquez simplement sur **Logging Settings** (Paramètres de journalisation) dans la table des matières.

Étape 2 Réglez le curseur **Internal Buffer** (Tampon interne) sur **On** (Activé) pour activer la mémoire tampon comme destination de journalisation.

Étape 3 Configurez les options de journalisation de la mémoire tampon interne :

- **Severity Level for Filtering All Events** (Niveau de gravité pour le filtrage de tous les événements) : sélectionnez le niveau de gravité. Les messages de ce niveau ou d'un niveau supérieur sont envoyés à la mémoire tampon interne.

- **Custom Logging Filter** (Filtre de journalisation personnalisé) : (facultatif) Si vous souhaitez effectuer un filtrage supplémentaire des messages, afin de n'obtenir que les messages qui vous intéressent, sélectionnez le event list filter (filtre de liste d'événements) qui définit les messages à générer. Si le filtre n'existe pas déjà, cliquez sur **Create New Event List Filter** (Créer un nouveau filtre de liste d'événements) et créez-le maintenant. Pour en savoir plus, consultez Configurer Event List Filters (Filtres de liste d'événements), à la page 793.
- **Buffer Size (Taille du tampon)** : taille du tampon interne dans lequel les messages syslog sont enregistrés. Lorsque la mémoire tampon est pleine, elle est remplacée. Par défaut, c'est de 4096 octets. La plage se situe entre 4096 et 52428800.

Étape 4 Cliquez sur **Save** (Enregistrer).

Configuration de la journalisation sur la console

Vous pouvez configurer le système pour envoyer des messages à la console. Ces messages apparaissent lorsque vous vous connectez à l'interface de ligne de commande sur le port de console. Vous pouvez aussi voir ces journaux dans une session SSH sur d'autres interfaces (y compris l'adresse de gestion) en utilisant la commande **show console-output**. En outre, vous pouvez voir ces messages en temps réel dans l'interface de ligne de commande de diagnostic, entrez **system support diagnostic-cli** depuis l'interface de ligne de commande principale.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis cliquez sur le lien **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation)**.

Si vous êtes déjà dans la page des paramètres système, cliquez simplement sur **Logging Settings** (Paramètres de journalisation) dans la table des matières.

Étape 2 Réglez le curseur **Console Filter** (Filtre de console) sur **On** (Activé) pour activer la console comme destination de journalisation.

Étape 3 Sélectionnez le niveau de **gravité**. Les messages à ce niveau ou à un niveau supérieur sont envoyés à la console.

Étape 4 Cliquez sur **Save** (Enregistrer).

Configurer Event List Filters (Filtres de liste d'événements)

Un event list filter (filtre de liste d'événements) est un filtre personnalisé que vous pouvez appliquer à une destination de journalisation pour contrôler les messages envoyés à la destination. Normalement, vous filtrez les messages pour une destination donnée uniquement en fonction de la gravité, mais vous pouvez utiliser un filtre pour affiner les messages envoyés en fonction d'une combinaison de classe d'événement, de gravité et d'identifiant de message (ID).

Vous n'utiliserez un filtre que si la limitation des messages par niveau de gravité est insuffisante pour vos besoins.

La procédure suivante explique comment créer le filtre à partir de la page **Objects** (Objets). Vous pouvez également créer un filtre lorsque vous configurez une destination de journalisation qui peut utiliser un filtre.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **Event List Filters (Filtres de liste d'événements)** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés du filtre :

- **Nom** : le nom de l'objet filtre.
- **Description** : ajoutez une description facultative.
- **Gravité et classe du journal** : si vous souhaitez filtrer par classe de message, cliquez sur **+**, sélectionnez un niveau de gravité pour le filtre de classe et cliquez sur **OK**. Ensuite, cliquez sur la flèche de liste déroulante dans le niveau de gravité, sélectionnez une ou plusieurs classes à filtrer à ce niveau de gravité, puis cliquez sur **OK**.

  Le système enverra des messages de journal système pour les classes de messages spécifiées uniquement si elles sont à ce niveau de gravité ou à un niveau supérieur. Vous pouvez ajouter au maximum une ligne pour chaque niveau de gravité.

  Si vous souhaitez filtrer toutes les classes à un niveau de gravité donné, laissez la liste de gravité vide et sélectionnez plutôt le niveau de gravité global pour la destination de journalisation lorsque vous l'activez.
- **Plage de Syslog/ID de message** : si vous souhaitez filtrer par l'ID de message syslog, saisissez un ID de message unique ou une plage de numéros d'ID pour laquelle vous souhaitez générer des messages. Séparez les chiffres de début et de fin par un tiret, par exemple 100 000-200 000. Les identifiants sont des numéros à 6 chiffres. Pour des ID de message spécifiques et les messages associés, consultez *Messages Syslog de Cisco Threat Defense* à l'adresse https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html.

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant sélectionner cet objet dans l'option de filtrage personnalisé pour les destinations de journalisation qui l'autorisent. Accédez à **Device (Périphérique)** > **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation)**.

Configuration du serveur DHCP

Un serveur DHCP fournit des paramètres de configuration réseau, tels que des adresses IP, aux clients DHCP. Vous pouvez configurer un serveur DHCP sur une interface pour fournir des paramètres de configuration aux clients DHCP sur le réseau connecté.

Un client DHCP IPv4 utilise une adresse de diffusion plutôt qu'une adresse de multidiffusion pour atteindre le serveur. Le client DHCP est à l'écoute des messages sur le port UDP 68; le serveur DHCP est à l'écoute des messages sur le port UDP 67. Le serveur DHCP ne prend pas en charge les demandes BOOTP.



Remarque Ne configurez pas de serveur DHCP sur un réseau sur lequel un serveur DHCP est déjà installé. Les deux serveurs seront en conflit, ce qui engendrera des résultats imprévisibles.

Avant de commencer

Les clients DHCP doivent être sur le même réseau que l'interface sur laquelle le serveur est activé. Autrement dit, il ne peut y avoir de routeur intermédiaire entre le serveur et le client, bien qu'il puisse y avoir un commutateur.

Si vous devez prendre en charge plusieurs réseaux et que vous ne souhaitez pas configurer un serveur DHCP sur chaque interface, vous pouvez configurer le relais DHCP pour transférer les demandes DHCP d'un réseau à un serveur DHCP hébergé sur un autre réseau. Dans ce cas, le serveur DHCP doit être hébergé sur un dispositif différent du réseau : vous ne pouvez pas configurer un serveur DHCP sur une interface et un relais DHCP sur une autre interface du même dispositif. Lorsque vous utilisez le relais DHCP, assurez-vous de configurer le serveur DHCP avec des ensembles d'adresses pour chaque espace d'adressage réseau géré par le serveur DHCP.

Pour configurer le relais DHCP, vous devez utiliser l'API Firepower Threat Defense. Utilisez la ressource dhcprelayservices.

Procédure

Étape 1 Cliquez sur **Device** (périphérique), puis sur le lien **System Settings (paramètres de système)** > **DHCP Server (serveur DHCP)**.

Si vous êtes déjà dans la page des paramètres système, cliquez simplement sur **DHCP Server (serveur DHCP)** dans la table des matières.

La page comporte deux onglets. Dans un premier temps, l'onglet **Configuration** affiche les paramètres globaux.

L'onglet **DHCP Servers (serveurs DHCP)** affiche les interfaces sur lesquelles vous avez configuré le serveur DHCP, indique si le serveur est activé et montre l'ensemble d'adresses pour le serveur.

Étape 2 Sous l'onglet **Configuration**, réglez la configuration automatique et les paramètres globaux.

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. Généralement, vous utiliseriez la configuration automatique si vous obtenez une adresse

en utilisant DHCP sur l'interface externe, mais vous pouvez choisir n'importe quelle interface qui obtient son adresse par le biais de DHCP. Si vous ne pouvez pas utiliser la configuration automatique, vous pouvez définir manuellement les options requises.

a) Cliquez sur **Enable Auto Configuration (activer la configuration automatique)** > **On (activé)** (le curseur doit être à droite) si vous souhaitez utiliser la configuration automatique, puis sélectionnez l'interface qui obtient son adresse par le biais de DHCP sous **From Interface** (de l'interface).

   Si vous configurez des routeurs virtuels, vous pouvez utiliser la configuration automatique du serveur DHCP sur une interface du routeur virtuel global uniquement. La configuration automatique n'est pas prise en charge pour les interfaces affectées à un routeur virtuel défini par l'utilisateur.

b) Si vous n'activez pas la configuration automatique ou si vous souhaitez remplacer l'un des paramètres configurés automatiquement, configurez les options globales suivantes. Ces paramètres seront envoyés aux clients DHCP sur toutes les interfaces qui hébergent le serveur DHCP.

   - **Primary WINS IP Address (adresse IP WINS principale)**, **Secondary WINS IP Address (adresse IP WINS secondaire)** : Les adresses des serveurs clients WINS (Windows Internet Name Service) que les clients doivent utiliser pour la résolution de noms NetBIOS.
   - **Primary DNS IP Address** (adresse IP du DNS primaire), **Secondary DNS IP Address**(adresse IP du DNS secondaire) : Les adresses des serveurs DNS (Domain Name System) que les clients doivent utiliser pour la résolution des noms de domaine. Cliquez sur **Use OpenDNS** si vous souhaitez configurer les serveurs DNS publics OpenDNS. Cliquez sur le bouton pour charger les adresses IP appropriées dans les champs.

c) Cliquez sur **Save** (Enregistrer).

Étape 3 Cliquez sur l'onglet **DHCP Servers** (serveurs DHCP) et configurez les serveurs.

a) Effectuez l'une des opérations suivantes :

   - Pour configurer le serveur DHCP pour une interface qui n'est pas déjà répertoriée, cliquez sur **+**.
   - Pour modifier un serveur DHCP existant, cliquez sur l'icône de modification () du serveur.

   Pour supprimer un serveur, cliquez sur l'icône de la corbeille () du serveur.

b) Configurez les propriétés du serveur :

   - **Enable DHCP Server (activer le serveur DHCP)** : Cette option permet d'activer le serveur. Vous pouvez configurer le serveur, mais laissez-le désactivé jusqu'à ce que vous soyez prêt à l'utiliser.
   - **Interface** : Sélectionnez l'interface sur laquelle vous allez fournir les adresses DHCP aux clients. L'interface doit avoir une adresse IP statique; vous ne pouvez pas utiliser DHCP pour obtenir l'adresse de l'interface si vous souhaitez exécuter un serveur DHCP sur l'interface. Pour les groupes de ponts, vous configurez le serveur DHCP sur l'interface BVI (Bridge Virtual Interface), et non les interfaces membres, et le serveur fonctionne sur toutes les interfaces membres.

     Vous ne pouvez pas configurer le serveur DHCP sur Diagnostic l'interface; configurez-le plutôt sur l'interface de gestion, dans la page **Device (dispositif)** > **System Settings (paramètres système)** > **Management Interface (dispositif de gestion)**.
   - **Address Pool (ensemble d'adresses)** : La plage des adresses IP (de la plus basse à la plus élevée) que le serveur est autorisé à fournir aux clients qui demandent une adresse. Indiquez les adresses de début et de fin de l'ensemble, séparées par un tiret. Par exemple, 10.100.10.12-10.100.10.250.

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, l'adresse de diffusion ou l'adresse réseau du sous-réseau.

La taille de l'ensemble se limite à 256 adresses par ensemble sur l'appareil Firepower Threat Defense. Si la plage d'adresses est supérieure à 253 adresses, le masque de réseau de l'interface Firepower Threat Defense ne peut pas être une adresse de classe C (par exemple, 255.255.255.0) et doit être plus grand, par exemple, 255.255.254.0.

c) Cliquez sur **OK**.

Configurer le DNS

Les serveurs du système de noms de domaine (DNS) sont utilisés pour transformer les noms d'hôtes en adresses IP. Vous configurez les serveurs DNS lors de la configuration initiale du système, et ces serveurs s'appliquent aux interfaces de données et de gestion. Vous pouvez les modifier après la configuration et utiliser des ensembles distincts de serveurs pour les interfaces de données et de gestion.

Vous devez au minimum configurer le DNS pour l'interface de gestion. Vous devez également configurer le DNS pour les interfaces de données si vous souhaitez utiliser des règles de contrôle d'accès basées sur FQDN ou si vous souhaitez utiliser les noms d'hôte dans les commandes CLI telles que **ping**.

La configuration du DNS est un processus en deux étapes : vous configurez les groupes DNS, puis vous configurez le DNS sur les interfaces.

Les rubriques suivantes expliquent plus en détail le processus.

Configuration des groupes DNS

Les groupes DNS (Domain Name System) définissent une liste de serveurs DNS et certains attributs associés. Vous pouvez configurer le DNS séparément sur les interfaces de gestion et de données. Les serveurs du système de noms de domaine (DNS) résolvent les noms de domaine complets (FQDN), tels que www.exemple.com, en adresses IP.

Après avoir terminé l'assistant de configuration du périphérique, vous aurez l'un des groupes DNS suivants définis par le système, ou les deux :

- CiscoUmbrellaDNSServerGroup : ce groupe comprend les adresses IP des serveurs DNS disponibles avec Cisco Umbrella. Si vous avez sélectionné ces serveurs lors de la configuration initiale, il s'agit du seul groupe défini par le système. Vous ne pouvez pas modifier le nom ou la liste de serveurs dans ce groupe, mais vous pouvez modifier les autres propriétés.
- CustomDNSServerGroup : si vous ne sélectionnez pas les serveurs Umbrella lors de la configuration du périphérique, le système crée ce groupe avec votre liste de serveurs. Vous pouvez modifier n'importe quelle propriété dans ce groupe.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **DNS Groups** (Groupes DNS) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un groupe, cliquez sur le bouton **Add Group** (ajouter un groupe) ( ).
- Pour modifier un groupe, cliquez sur l'icône de modification ( ) du groupe.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés suivantes :

- **Nom** : le nom du groupe de serveurs DNS. Le nom DefaultDNS est réservé : vous ne pouvez pas l'utiliser.
- **Adresses IP DNS** : saisissez l'adresse IP d'un serveur DNS. Cliquez sur **Add Another DNS IP Address** (Ajouter une autre adresse IP DNS) pour configurer plusieurs serveurs. Si vous souhaitez supprimer une adresse de serveur, cliquez sur l'icône de suppression ( ) en regard de l'adresse.

  La liste est en ordre de priorité : le premier serveur de la liste est toujours utilisé et les serveurs suivants ne sont utilisés que si les serveurs précédents ne répondent pas. Vous pouvez configurer jusqu'à 3 serveurs.
- Dans **Domain Search Name** (Nom de recherche du domaine), saisissez le nom de domaine de votre réseau, par exemple, exemple.com. Ce domaine est ajouté aux noms d'hôte qui ne sont pas complets, par exemple, serverA au lieu de serverA.example.com. Le nom doit comporter moins de 63 caractères pour que le groupe puisse être utilisé pour les interfaces de données.
- **Nombre de tentatives** : le nombre de tentatives, de 0 à 10, pour réessayer la liste des serveurs DNS lorsque le système ne reçoit pas de réponse. La valeur par défaut est 2. Ce paramètre s'applique uniquement aux groupes DNS utilisés sur les interfaces de données.
- **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 le système réessaie la liste des serveurs, ce délai est doublé. Ce paramètre s'applique uniquement aux groupes DNS utilisés sur les interfaces de données.

Étape 4 Cliquez sur **OK**.

Configuration DNS pour les données et le trafic de gestion

Les serveurs du système de noms de domaine (DNS) sont utilisés pour transformer les noms d'hôtes en adresses IP. Il existe deux paramètres de serveur DNS qui s'appliquent à différents types de trafic : le trafic de données et le trafic spécial de gestion. Le trafic de données comprend tous les services qui utilisent des noms de domaine complets pour lesquels une recherche DNS est nécessaire, comme les règles de contrôle d'accès et le VPN d'accès à distance. Le trafic spécial de gestion comprend le trafic provenant de l'interface de gestion, tel que Smart Licensing et les mises à jour de la base de données.

Si vous utilisez l'assistant de configuration de l'interface de ligne de commande, vous configurez les serveurs DNS de gestion lors de la configuration système initiale. Vous pouvez également définir les serveurs DNS

de données et de gestion dans l'assistant de configuration Gestionnaire de périphériques de pare-feu. Vous pouvez modifier les valeurs par défaut des serveurs DNS en utilisant la procédure suivante.

Vous pouvez également modifier la configuration DNS de gestion dans l'interface de ligne de commande à l'aide des commandes **configure network dns servers** et **configure network dns searchdomains**. Si les interfaces de données et de gestion utilisent le même groupe DNS, le groupe est mis à jour et lors de votre prochain déploiement, les modifications sont également appliquées aux interfaces de données.

Pour déterminer l'interface correcte pour les communications du serveur DNS, le Firewall Threat Defense utilise une recherche de routage, mais la table de routage utilisée dépend des interfaces pour lesquelles vous activez le DNS. Pour en savoir plus, reportez-vous aux paramètres de l'interface ci-dessous.

Si vous avez des problèmes avec la résolution DNS, consultez :

- Dépannage des problèmes généraux de DNS, à la page 800
- Dépannage du DNS pour l'interface de gestion, à la page 858

Avant de commencer

- Assurez-vous d'avoir créé un ou plusieurs groupe(s) de serveurs DNS. Pour plus d'informations sur les instructions, consultez Configuration des groupes DNS, à la page 797
- Assurez-vous que le périphérique Firewall Threat Defense dispose des routes statiques ou dynamiques appropriées pour accéder aux serveurs DNS.

Procédure

Étape 1 Cliquez sur **Device** (Dispositif), puis sur le lien **System Settings (Paramètres système)** > **DNS Server (Serveur DNS)**.

Si vous êtes déjà sur la page **System Settings** (Paramètres système), cliquez sur **DNS Server** (Serveur DNS) dans la table des matières.

Étape 2 Configurez le DNS pour l'**interface de données**.

a) Activer les recherches DNS sur toutes les interfaces ou sur des interfaces spécifiques. Ces choix affectent également les tables de routage utilisées.

Notez que l'activation des recherches DNS sur une interface n'est pas la même chose que la spécification de l'interface source pour les recherches. Le périphérique utilise toujours une recherche de routage pour déterminer l'interface source.

- **Aucune interface sélectionnée** : active les recherches DNS sur toutes les interfaces, y compris les interfaces de gestion et les interfaces de gestion uniquement. Le périphérique vérifie la table de routage des données et, si aucune route n'est trouvée, il revient à la table de routage de gestion uniquement.
- Interfaces sélectionnées, mais pas l'interface Diagnostic ou une interface de gestion uniquement : active les recherches DNS sur les interfaces spécifiées. Le périphérique contrôle la table de routage des données uniquement.
- Interfaces sélectionnées plus l'interface Diagnostic ou une interface de gestion uniquement : active les recherches DNS sur les interfaces spécifiées. Le périphérique vérifie la table de routage des données et, si aucune route n'est trouvée, revient à la table de routage de gestion uniquement.

- Uniquement l'interface Diagnostic ou une interface réservée à la gestion sélectionnée : active les recherches DNS sur Diagnostic ou sur une interface réservée à la gestion uniquement. Le périphérique ne vérifie que la table de routage de gestion.

b) Sélectionnez le **groupe DNS** qui définit les serveurs à utiliser sur les interfaces de données. Si le groupe dont vous avez besoin n'est pas encore défini, cliquez sur **Create New DNS Group (Créer un nouveau groupe DNS)** et créez-le maintenant. Sélectionnez **None** (Aucun) si vous souhaitez empêcher les recherches sur les interfaces de données.

c) (Facultatif) Configurez les **paramètres DNS FQDN** si vous utilisez des objets réseau FQDN dans les règles de contrôle d'accès.

Ces options sont utilisées uniquement lors de la résolution d'objets FQDN et sont ignorées pour tout autre type de résolution DNS.

- **Temps d'interrogation** : durée, en minutes, du cycle d'interrogation utilisé pour résoudre les objets réseau FQDN en adresses IP. Les objets FQDN sont résolus uniquement s'ils sont utilisés dans la politique de contrôle d'accès. La minuterie détermine le délai maximal 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 peuvent 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.

- **Expiration** : nombre de minutes après l'expiration d'une entrée DNS (c'est-à-dire après la fin du TTL envoyé par le serveur DNS) durant lesquelles l'entrée demeure dans la table de consultation DNS avant d'être supprimée. 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 de 1 minute (c'est-à-dire que l'entrée est supprimée une minute après la fin de la TTL). La plage est comprise entre 1 et 65535 minutes.

d) Cliquez sur **Save** (enregistrer). Vous devez également déployer la configuration pour appliquer les modifications au périphérique.

Étape 3 Configurer DNS pour l'**interface de gestion**.

a) Sélectionnez le **groupe DNS** qui définit les serveurs à utiliser sur l'interface de gestion. Si le groupe dont vous avez besoin n'est pas encore défini, cliquez sur **Create New DNS Group** (Créer un nouveau groupe DNS) et créez-le maintenant.

b) Cliquez sur **Save** (enregistrer). Vous devez déployer des modifications pour mettre à jour les serveurs DNS de gestion.

Dépannage des problèmes généraux de DNS

Vous devez configurer séparément les serveurs DNS pour les interfaces de gestion et de données. Certaines fonctionnalités permettent la résolution de noms à l'aide de l'un ou l'autre type d'interface, mais pas des deux. Parfois, une fonctionnalité donnée utilise différentes méthodes de résolution en fonction de votre utilisation.

Par exemple, les commandes **ping** *hostname* et **ping interface** *interface_name hostname* utilisent les serveurs DNS de l'interface de données pour résoudre le nom, alors que la commande **ping system** *hostname* utilise les serveurs DNS de l'interface de gestion. Cela vous permet de tester la connectivité via des interfaces spécifiques et la table de routage.

Gardez cela à l'esprit lorsque vous rencontrez des problèmes de recherche de nom d'hôte.

Pour le dépannage de DNS pour l'interface de gestion, consultez également Dépannage du DNS pour l'interface de gestion, à la page 858.

Lorsque vous n'obtenez aucune résolution de nom

Voici quelques conseils de dépannage si vous n'obtenez tout simplement aucune résolution de nom.

- Vérifiez que vous avez configuré des serveurs DNS pour les interfaces de gestion et de données. Pour les interfaces de données, utilisez « Any » pour l'interface. Spécifiez les interfaces explicitement uniquement si vous ne souhaitez pas autoriser le DNS sur certaines interfaces.
- Si vous utilisez l'interface de diagnostic pour les recherches sur les interfaces de données, vérifiez que vous avez configuré une adresse IP sur l'interface. Les recherches nécessitent que l'interface dispose d'une adresse IP.
- Vous ne pouvez pas atteindre le serveur DNS par Diagnostic l'interface ou par une interface de gestion uniquement, car la recherche de voie de routage trouve une correspondance dans la table de routage de données, de sorte qu'il n'y a pas de retour à la table de routage de gestion uniquement. Si vous souhaitez utiliser l'interface Diagnostic, assurez-vous qu'il s'agit de la seule interface sélectionnée.
- Envoyez un message ping à l'adresse IP de chaque serveur DNS pour vérifier qu'elle est accessible. Utilisez les mots-clés **system** et **interface** pour tester des interfaces spécifiques. Si l'envoi du message ping échoue, vérifiez vos voies de routage statique et vos passerelles. Vous devrez peut-être ajouter des voies de routage statique pour les serveurs.
- Si l'envoi du message réussit, mais que la résolution de nom échoue, vérifiez vos règles de contrôle d'accès. Vérifiez que vous autorisez le trafic DNS (UDP/53) pour les interfaces par lesquelles les serveurs sont accessibles. Il est également possible que ce trafic soit bloqué par un périphérique qui se trouve entre votre système et le serveur DNS. Vous devrez peut-être utiliser différents serveurs DNS.
- Si l'envoi du message réussit, que les voies de routage sont adéquates et que les règles de contrôle d'accès ne posent pas le problème, considérez que le serveur DNS ne peut peut-être pas être mis en correspondance avec le nom de domaine complet. Vous devrez peut-être faire appel à différents serveurs.

Lorsque vous obtenez une mauvaise résolution de nom

Si vous obtenez une résolution de nom, mais que l'adresse IP d'un nom n'est pas exacte, il y a peut-être un problème de mise en mémoire cache. Ce problème toucherait uniquement aux fonctionnalités basées sur l'interface de données, telles que les objets réseau du nom de domaine complet utilisés dans les règles de contrôle d'accès.

Le système dispose d'une mémoire cache locale d'informations DNS obtenues lors de précédentes recherches. Lorsqu'une nouvelle recherche est requise, le système fait d'abord des recherches dans la mémoire cache locale. 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 serveurs DNS. 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.

Chaque recherche a une durée de vie définie par le serveur DNS et expire automatiquement de la mémoire de cache. En outre, le système actualise périodiquement la valeur des noms de domaine complets qui sont utilisés dans les règles de contrôle d'accès. Au minimum, cette actualisation a lieu à l'intervalle du délai d'interrogation (par défaut, toutes les 4 heures), mais elle peut être plus fréquente en fonction de la durée de vie de l'entrée.

Utilisez les commandes **show dns-hosts** et **show dns** pour consulter la mémoire cache locale. Si les adresses IP d'un nom de domaine complet sont incorrectes, vous pouvez utiliser la commande **dns update** [**host** *hostname*] pour forcer le système à actualiser les informations. Si vous utilisez la commande sans spécifier d'hôte, tous les noms d'hôte sont actualisés.

Vous pouvez supprimer les informations mises en cache en utilisant les commandes **clear dns** [**host** *fqdn*] et **clear dns-hosts cache**.

Configuration de l'interface de gestion

L'interface de gestion est une interface virtuelle reliée au port de gestion physique. Notez que l'interface physique comprend également l'interface virtuelle de diagnostic, que vous pouvez configurer sur la page **Interfaces** avec d'autres interfaces physiques. Reportez-vous àInterface de gestion/dépistage, à la page 253 pour obtenir plus de renseignements sur l'interface de diagnostic.

L'interface de gestion a deux utilisations :

- Vous pouvez ouvrir des connexions Web et SSH à l'adresse IP et configurer l'appareil au moyen de l'interface.
- Le système obtient les licences intelligentes et les mises à niveau de la base de données grâce à cette adresse IP.

Si vous utilisez l'assistant de configuration de l'interface de ligne de commande, vous configurez l'adresse de gestion et la passerelle du périphérique lors de la configuration système initiale. Si vous utilisez l'assistant de configuration Gestionnaire de périphériques de pare-feu, l'adresse de gestion et la passerelle restent les valeurs par défaut.

Si nécessaire, vous pouvez modifier ces adresses au moyen de Gestionnaire de périphériques de pare-feu. Vous pouvez également modifier l'adresse de gestion et la passerelle dans l'interface de ligne de commande à l'aide des commandes **configure network ipv4 manual** et **configure network ipv6 manual**. Pour restaurer les paramètres par défaut de l'interface de gestion, utilisez la commande **configure network** {**ipv4** | **ipv6**} **dhcp-dp-route**.

Vous pouvez définir des adresses statiques ou obtenir une adresse au moyen de DHCP si un autre périphérique du réseau de gestion agit en tant que serveur DHCP. Pour la plupart des plateformes, l'interface de gestion obtient une adresse IP de DHCP par défaut.

Mise en garde Si vous modifiez l'adresse à laquelle vous êtes actuellement connecté, vous perdrez l'accès à Gestionnaire de périphériques de pare-feu (ou à l'interface de ligne de commande) lorsque vous enregistrerez les modifications, car elles s'appliqueront immédiatement. Vous devrez vous reconnecter à l'appareil. Assurez-vous que la nouvelle adresse est valide et disponible sur le réseau de gestion.

Procédure

Étape 1 Cliquer sur **l'appareil**, puis cliquez sur **Systems Settings (paramètres systèmes) du lien de > l'interface de gestion**.

Si vous êtes déjà sur la page **System Settings** cliquez sur **interface de gestion** dans la table des matières

Étape 2 Choisissez la façon dont vous souhaitez définir la passerelle de gestion.

La passerelle détermine comment le système peut accéder à Internet pour obtenir des licences intelligentes, des mises à niveau de bases de données (telles que VDB, règle, géolocalisation, URL) et pour atteindre les serveurs DNS et NTP de gestion. Choisissez à partir de ces options :

Options IP statiques :

- **Utiliser les interfaces de données comme passerelle :** sélectionnez cette option si vous n'avez pas de réseau de gestion distinct connecté à l'interface de gestion. Le trafic est acheminé vers Internet en fonction de la table de routage, en passant généralement par l'interface externe. Cette option n'est pas prise en charge sur les appareils Firewall Threat Defense Virtual.
- **Utiliser des passerelles uniques pour l'interface de gestion :** spécifier des passerelles uniques (ci-dessous) pour IPv4 et IPv6 si vous disposez d'un réseau de gestion distinct connecté à l'interface de gestion.

Options IP de DHCP :

- **Utiliser des passerelles uniques pour l'interface de gestion avec des interfaces de secours vers les données : si le serveur DHCP fournit une passerelle, le système achemine le trafic de gestion vers la passerelle via l'interface de gestion.** Si le serveur DHCP ne fournit pas de passerelle, le système achemine le trafic de gestion en fonction de la table de tourage de l'interface de données, envoyant généralement le trafic au moyen de l'interface externe. Cette option n'est pas prise en charge sur les appareils Firewall Threat Defense Virtual.
- **Utiliser des passerelles uniques pour l'interface de gestion (pas de secours) : le système achemine le trafic de gestion via l'interface de gestion vers la passerelle fournie par le serveur DHCP.** Si le serveur DHCP ne fournit pas de passerelle, le système ne pourra atteindre que les hôtes locaux sur l'interface de gestion. Pour acheminer au moyen des interfaces de données, choisir l'option de secours.

Étape 3 Configurez l'adresse de gestion, le masque de sous-réseau ou le préfixe IPv6 et la passerelle (si nécessaire) pour IPv4, IPv6 ou les deux.

Vous devez configurer au moins un ensemble de propriétés. Laissez un ensemble vide pour désactiver cette méthode d'adressage.

Sélectionnez le type **de** > **DHCP**pour obtenir l'adresse et la passerelle au moyen de la configuration automatique DHCP ou IPv6.

Étape 4 (Facultatif) Si vous configurez une adresse IPv4 statique, configurez un serveur DHCP sur l'interface.

Si vous configurez un serveur DHCP sur l'interface de gestion, les clients du réseau de gestion peuvent obtenir leur adresse à partir du pool DHCP. Cette option n'est pas prise en charge sur les appareils Firewall Threat Defense Virtual.

a) Cliquez **Enable DHCP Server (activer le serveur DHCP)** > **sur**.
b) Entrer **le pool d'adresses** pour le serveur.

Le pool d'adresses est la plage d'adresses IP, de la plus basse à la plus haute, que le serveur est autorisé à fournir aux clients qui demandent une adresse. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'adresse de gestion et ne peut pas inclure : l'adresse IP de l'interface elle-même, l'adresse de diffusion ou l'adresse réseau du sous-réseau. Indiquez les adresses de début et de fin de l'ensemble, séparées par un tiret. Par exemple, 192.168.45.46-192.168.45.254.

Étape 5 Cliquez sur **Save** (Enregistrer), lisez l'avertissement, puis cliquez sur **OK**.

Configurer le nom d'hôte du périphérique.

Vous pouvez modifier le nom d'hôte du périphérique.

Vous pouvez également modifier le nom d'hôte dans l'interface de ligne de commande à l'aide de la commande **configure network hostname**.

Mise en garde Si vous modifiez le nom d'hôte lorsque vous êtes connecté au système en utilisant ce nom, vous perdrez l'accès à Gestionnaire de périphériques de pare-feu lorsque vous enregistrerez les modifications, car elles s'appliquent immédiatement. Vous devrez vous reconnecter à l'appareil.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur le lien **System Settings (Paramètres du système)** > **Hostname (Nom d'hôte)**.

Si vous êtes déjà sur la page des paramètres système, cliquez simplement sur **Hostname** (Nom d'hôte) dans la table des matières.

Étape 2 Entrez un nouveau nom d'hôte.

Étape 3 Cliquez sur **Save** (enregistrer).

La modification du nom d'hôte est immédiatement appliquée à certains processus système. Cependant, vous devez déployer les modifications pour terminer la mise à jour afin que le même nom soit utilisé par tous les processus du système.

Protocole de temps réseau (NTP)

Vous devez configurer les serveurs Network Time Protocol (NTP) pour définir l'heure sur le système. Vous configurez les serveurs NTP lors de la configuration initiale du système, mais vous pouvez les modifier à l'aide de la procédure suivante. Si vous avez des problèmes avec la connexion NTP, consultez Dépannage du protocole NTP, à la page 857.

Le périphérique Firewall Threat Defense prend en charge NTPv4.

Remarque Pour le Firepower 4100/9300, vous ne définissez pas le NTP par l'intermédiaire de Gestionnaire de périphériques de pare-feu. Configurez le NTP dans FXOS.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis cliquez sur le lien **System Settings (Paramètres système)** > **Time Services (Services de temps)**.

Si vous êtes déjà sur la page System Settings (Paramètres système), cliquez simplement sur **Time Services (Services de temps)** dans la table des matières.

Étape 2 Dans **NTP Time Server** (Serveur de temps NTP), sélectionnez si vous souhaitez utiliser vos propres serveurs de temps ou ceux de Cisco.

- **Default NTP Servers (Serveurs NTP par défaut)**—Si vous sélectionnez cette option, la liste des serveurs affiche les noms des serveurs utilisés pour le NTP.
- **User-Defined NTP Servers (Serveurs NTP définis par l'utilisateur)**—Si vous sélectionnez cette option, saisissez le nom de domaine complet ou l'adresse IPv4 ou IPv6 du serveur NTP que vous souhaitez utiliser. Par exemple, ntp1.exemple.com ou 10.100.10.10. Vous pouvez ajouter jusqu'à 3 serveurs NTP.

Étape 3 Cliquez sur **Save** (Enregistrer).

Configuration du protocole Precision Time Protocol (PTP) (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 le périphérique Firewall Threat Defense pour qu'il soit une horloge transparente. Le périphérique Firewall Threat Defense ne synchronise pas son horloge avec les horloges PTP. Le périphérique Firewall Threat Defense 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 destinés à fonctionner ensemble. Ainsi, vous pouvez configurer plusieurs domaines PTP, puis configurer chaque périphérique non PTP pour utiliser les horloges PTP d'un domaine spécifique.

Avant de commencer

Déterminez le numéro de domaine configuré sur les horloges PTP que le périphérique doit utiliser. Déterminez également les interfaces par lesquelles le système peut atteindre les horloges PTP du domaine.

Voici des consignes pour la configuration du PTP :

- Cette fonctionnalité est uniquement disponible sur le périphérique Cisco ISA 3000.
- Cisco PTP prend uniquement en charge les messages PTP en multidiffusion.
- 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 de données Ethernet physiques, qu'elles soient autonomes ou membres d'un groupe de ponts. Elle n'est pas prise en charge sur l'interface de gestion, les sous-interfaces, les EtherChannels, les interfaces virtuelles de pont (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. Le trafic PTP est identifié par les ports de destination UDP 319 et 320 et par l'adresse IP de destination 224.0.1.129, donc toute règle de contrôle d'accès qui autorise ce trafic devrait fonctionner.
- Lorsque les paquets PTP circulent entre des interfaces routées, vous devez activer le routage de multidiffusion et chaque interface doit rejoindre le groupe de multidiffusion IGMP 224.0.1.129. Lorsque les paquets PTP circulent entre des interfaces du même groupe de ponts, vous n'avez pas besoin d'activer le routage de multidiffusion ni de configurer le groupe IGMP.

Procédure

Étape 1 Vérifiez la configuration des interfaces orientées horloge PTP.

La configuration par défaut place toutes les interfaces dans le même groupe de ponts, mais vous pouvez retirer des interfaces du groupe de ponts. Il est important de déterminer si les interfaces sont routées ou membres de groupes de ponts, car vous devez les configurer différemment par rapport aux groupes IGMP de multidiffusion.

La procédure suivante explique comment déterminer quelles interfaces font partie du groupe de ponts. Vérifiez si les interfaces que vous configurez pour le PTP sont membres de groupes de ponts.

a) Cliquez sur **View All Interfaces** (Afficher toutes les interfaces) dans **Device (Périphérique)** > **Interfaces**.
b) Recherchez les interfaces dans la liste et vérifiez la colonne Mode. BridgeGroupMember signifie qu'il fait partie d'un groupe de ponts, sinon il doit être routé.

Étape 2 Cliquez sur **Device (Périphérique)**, puis cliquez sur le lien **System Settings (Paramètres système)** > **Time Services (Services de temps)**.

Si vous êtes déjà sur la page **System Settings** (Paramètres du système, cliquez simplement sur **Time Services** (Services de temps) dans la table des matières.

Étape 3 Configurez les paramètres PTP :

- **Domain Number** (Numéro de domaine) : numéro de domaine configuré sur les périphériques PTP de votre réseau, de 0 à 255. Les paquets reçus dans un domaine différent sont traités comme des paquets de multidiffusion ordinaires et ne subissent aucun traitement PTP.
- **Clock Mode** (Mode horloge) : sélectionnez **EndToEndTransparent**. Vous ne pouvez utiliser le périphérique que comme horloge transparente PTP.

Vous pouvez également sélectionner **Forward**, mais cela revient essentiellement à ne pas configurer PTP. Le numéro de domaine est ignoré. Les paquets PTP passent par le périphérique en fonction de la table de routage du trafic de multidiffusion. Il s'agit de la configuration PTP par défaut.

- **Interfaces** : sélectionnez toutes les interfaces par lesquelles le système peut se connecter à l'horloge PTP dans votre réseau. Le protocole PTP est activé uniquement sur ces interfaces.

Étape 4 Cliquez sur **Save** (enregistrer).

Étape 5 Si certaines des interfaces que vous avez sélectionnées sont des interfaces routées, c'est-à-dire qu'elles ne sont pas membres d'un groupe de ponts, vous devez utiliser FlexConfig (FlexConfig) pour activer le routage de multidiffusion et joindre les interfaces routées au groupe IGMP approprié.

N'effectuez pas cette étape si toutes les interfaces sélectionnées sont membres d'un groupe de ponts. Vous obtiendrez un échec de déploiement si vous tentez de configurer IGMP sur un membre d'un groupe de ponts.

a) Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

b) Cliquez sur **FlexConfig** > **FlexConfig Objects** (Objets FlexConfig) dans la table des matières de Advanced Configuration (Configuration avancée).

c) Créez l'objet nécessaire pour activer le routage de multidiffusion et configurer la jonction IGMP pour les interfaces routées.

Voici le modèle de base pour l'objet. Dans cet exemple, GigabitEthernet1/2 est la seule interface routée sur laquelle vous activez le protocole PTP. Modifiez le nom matériel de l'interface, au besoin, et si vous avez plusieurs interfaces routées, répétez les commandes **interface** et **igmp** pour chaque interface supplémentaire.

La commande **igmp** rejoint le groupe IGMP 224.0.1.129. Il s'agit de l'adresse IP correcte pour toutes les interfaces, quelle que soit l'adresse réseau.

```
multicast-routing
interface GigabitEthernet1/2
 igmp join-group 224.0.1.129
```

Le modèle de négation ressemblerait à ce qui suit :

```
no multicast-routing
interface GigabitEthernet1/2
 no igmp join-group 224.0.1.129
```

d) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières, ajoutez cet objet à la politique FlexConfig, puis cliquez sur **Save** (Enregistrer).

Vérifiez que l'aperçu affiche les commandes attendues provenant de votre objet.

Prochaine étape

Après avoir déployé les modifications, vous pouvez vérifier les paramètres PTP. Depuis la console d'interface de ligne de commande Gestionnaire de périphériques de pare-feu, ou à partir d'une session SSH ou Console, exécutez les différentes commandes **show ptp**. Par exemple, si vous avez configuré le protocole PTP pour le domaine 10 uniquement sur GigabitEthernet1/2, la sortie peut ressembler à ce qui suit :

```
> show ptp clock
```

```
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
  PTP version: 2
  Port state: Disabled
```

Configuration du serveur mandataire HTTP pour les connexions de gestion

S'il n'y a pas de connexion directe entre le système et Internet, vous pouvez configurer un serveur mandataire HTTP pour l'interface de gestion. Le système utilisera ensuite le serveur mandataire pour toutes les connexions de gestion, y compris les connexions à Gestionnaire de périphériques de pare-feu et du système à Cisco pour le téléchargement des mises à jour de la base de données.

Vous pouvez également configurer un serveur mandataire HTTP dans l'interface de ligne de commande Firewall Threat Defense à l'aide de la commande **configure network http-proxy**.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien **System Settings (Paramètres système)** > **HTTP Proxy**.

Si vous êtes déjà sur la page **System Settings** (Paramètres système), cliquez simplement sur **HTTP Proxy** dans la table des matières.

Étape 2 Cliquez sur la bascule pour activer le serveur mandataire, puis configurez les paramètres du serveur mandataire :

- **HTTP Proxy** : adresse IP du serveur mandataire.
- **Port** : numéro de port auquel le serveur mandataire est configuré pour surveiller les connexions HTTP.

- **Utiliser l'authentification du serveur mandataire** : sélectionnez cette option si le serveur est configuré pour exiger l'authentification pour les connexions par serveur mandataire. Si vous sélectionnez cette option, saisissez également le **nom d'utilisateur** et **le mot de passe** d'un compte qui peut se connecter au serveur mandataire.

Étape 3 Cliquez sur **Save** (Enregistrer), puis confirmez que vous souhaitez apporter la modification.

Vos modifications sont appliquées immédiatement. Une tâche de déploiement n'est pas nécessaire.

Comme vous modifiez la façon dont le système effectue les connexions de gestion, vous perdrez votre connexion à Gestionnaire de périphériques de pare-feu. Attendez quelques minutes que la modification soit terminée, puis actualisez la fenêtre de votre navigateur et connectez-vous de nouveau.

Configuration de Cisco Cloud Services

Vous pouvez vous inscrire aux services en nuage pour pouvoir utiliser diverses applications en nuage, comme Contrôle de Security Cloud, Cisco Threat Response et le Cisco Success Network.

Une fois enregistré dans le nuage, la page affiche l'état de l'enregistrement et le type de location, ainsi que le nom du compte sous lequel l'appareil est enregistré.

Procédure

Étape 1 Cliquez **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Cisco Cloud Services**.

Si vous êtes déjà sur la page **System Settings (paramètres système)**, cliquez simplement sur **Cisco Cloud Services** dans la table des matières.

Si votre appareil n'est pas enregistré, cette page affiche les méthodes d'enregistrement pour l'enregistrement dans le nuage de Cisco. Après votre inscription au nuage, vous serez en mesure d'activer ou de désactiver les services en nuage individuels.

Étape 2 Pour vous inscrire au nuage de Cisco (en mode d'évaluation ou après vous être désinscrit de Cisco Cloud services), sélectionnez l'une des options suivantes :

- **Security**/Contrôle de Security Cloud **Account Security** (Sécurité/ Sécurité du compte/Compte SCC) — Vous pouvez utiliser l'une des méthodes suivantes :
  - **Inscription automatique auprès de la location de Contrôle de Security Cloud** (Firepower 1000, 2100, uniquement). Vous pouvez utiliser l'inscription automatique au lieu d'obtenir une clé d'inscription. Tout d'abord, allez à Contrôle de Security Cloud et ajoutez l'appareil à l'aide du numéro de série de l'appareil. Ensuite, dans le Gestionnaire de périphériques de pare-feu, activez cette case à cocher et lancez l'inscription. Obtenez le numéro de série sur le châssis de l'appareil ou sur le bon de livraison. Pour FXOS, vous pouvez aller dans l'interface de ligne de commande FXOS et utiliser la commande **show chassis detail** pour récupérer le numéro de série correct, étiqueté Serial (SN). Notez que la commande Firewall Threat Defense **show serial-number** fournit un numéro de série différent, ce qui n'est pas recommandé pour l'enregistrement Contrôle de Security Cloud.

- Connectez-vous à votre compte Contrôle de Security Cloud ou à un autre compte de sécuritéet générez une clé d'enregistrement. Revenez ensuite à cette page, sélectionnez votre**Cisco Cloud Services Region (région de Cisco Cloud Services)**, et collez votre **Registration Key (clé d'enregistrement)**.

  Vous pouvez également activer **Contrôle de Security Cloud** et **Cisco Success Network** à ce stade. Ceux-ci sont activés par défaut.

- **Licence Smart** : (uniquement si vous ne l'utilisez pas.)Contrôle de Security Cloud Cliquez sur le lien pour accéder à la page de licences Smart et vous inscrire auprès de CSSM. L'enregistrement auprès du CSSM enregistre également l'appareil auprès de Cloud Services .

  Remarque
  Si vous vous êtes désinscrit de Cloud Services, alors l'approche Smart License de l'inscription comporte quelques étapes supplémentaires. Dans ce cas, sélectionnez **Cloud Services Region (région Cisco Cloud Services)**, puis cliquez sur **Register (inscription)**. Lisez la divulgation et cliquez sur **Accept (accepter)**.

Étape 3 Une fois que vous vous êtes inscrit aux services en nuage, vous pouvez activer ou désactiver des fonctionnalités selon vos besoins. Consultez les rubriques suivantes:

- Activation ou désactivation Contrôle de Security Cloud (Mode gestionnaire d'appareil existant)
- Connexion à Cisco Success Network, à la page 811
- Envoi d'événements à Cisco Cloud, à la page 812
- Se désinscrire de Cisco Cloud services, à la page 813

Activation ou désactivation Contrôle de Security Cloud (Legacy Device Manager Mode (mode de gestionnaire d'appareil existant))

Remarque Cette section s'applique uniquement à l'ancien mode de gestionnaire d'appareils dans Contrôle de Security Cloud, et non au centre de gestion en nuage.

Si vous vous êtes inscrit aux services en nuage à l'aide d'une clé d'enregistrement de Contrôle de Security Cloud, comme recommandé dans Configuration de Cisco Cloud Services, à la page 809, l'appareil est déjà enregistré avec Contrôle de Security Cloud. Ensuite, vous pouvez désactiver ou réactiver la connexion comme vous le souhaitez.

Si l'appareil est enregistré auprès de Cisco Cloud Services à l'aide de licences intelligentes, vous aurez des problèmes si vous activez Contrôle de Security Cloud : l'appareil n'apparaîtra pas dans l'inventaire Contrôle de Security Cloud. Nous vous recommandons fortement de désinscrire d'abord l'appareil de Cisco Cloud services; sélectionnez **Unregister Cloud Services (annuler l'enregistrement de Cisco Cloud services)** dans la liste déroulante de l'équipement ( ). Après vous être désinscrit, obtenez un jeton d'enregistrement auprès de Contrôle de Security Cloud et réinscrivez-vous à l'aide du jeton et de votre compte de sécurité, comme expliqué dans Configuration de Cisco Cloud Services, à la page 809.

pour obtenir plus de renseignements sur le fonctionnement de la gestion du cloud, consultez le portailContrôle de Security Cloud (http://www.cisco.com/go/cdo) ou demandez au revendeur ou au partenaire avec lequel vous travaillez.

Avant de commencer

Si vous avez l'intention de configurer la haute disponibilité, vous devez enregistrer les deux périphériques que vous utiliserez dans le groupe de haute disponibilité.

Procédure

Étape 1 Cliquez **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Cisco Cloud Services**.

Si vous êtes déjà sur la page System Settings (paramètres système), cliquez simplement sur **Cisco Cloud Services** dans la table des matières.

Étape 2 Cliquez sur le bouton **Enable**/**Disable** (activer/Désactiver) pour que la fonctionnalité Contrôle de Security Cloud modifie le paramètre en conséquence.

Connexion à Cisco Success Network

Lorsque vous enregistrez l'appareil, vous décidez si vous souhaitez activer la connexion à Cisco Success Network. Consultez Enregistrement de l'appareil, à la page 93.

En activant le Cisco Success Network, vous fournissez à Cisco des informations et des statistiques d'utilisation qui sont essentielles pour que Cisco puisse vous fournir une assistance technique. Ces informations permettent également à Cisco d'améliorer le produit et de vous informer des fonctionnalités disponibles inutilisées afin de maximiser la valeur du produit sur votre réseau.

Lorsque vous activez la connectivité, votre appareil établit une connexion sécurisée avec Cisco Cloud afin que votre appareil puisse participer à des offres de services supplémentaires de Cisco, tels que les Services d'assistance technique de Cisco, la gestion du cloud et les services de surveillance. Votre appareil établira et maintiendra cette connectivité sécurisée à tout moment. pour obtenir plus de renseignements sur la déconnexion complète du nuage, consultez Se désinscrire de Cisco Cloud services, à la page 813.

Une fois que vous avez enregistré le périphérique, vous pouvez modifier le paramètre du Cisco Success Network.

Remarque Lorsque le système envoie des données à Cisco, la liste des tâches affiche une tâche de télémétrie.

Avant de commencer

Pour activer le Cisco Success Network, l'appareil doit être inscrit dans le nuage. Pour inscrire le périphérique, enregistrez-le auprès de Cisco Smart Software Manager (sur la page Smart Licensing), en sélectionnant l'option Cisco Success Network lors de l'inscription, ou inscrivez-le Contrôle de Security Clouden entrant une clé d'inscription (mode gestionnaire d'appareil hérité dans CDO Contrôle de Security Clouduniquement).

Remarque Si vous activez le Cisco Success Network sur l'unité active dans un groupe à haute disponibilité, vous activez également la connexion sur l'unité en veille.

Procédure

Étape 1 Cliquez **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Cisco Cloud Services**.

Si vous êtes déjà sur la page System Settings (paramètres système), cliquez simplement sur **Cisco Cloud Services** dans la table des matières.

Étape 2 Cliquez sur le contrôle **Enable (activer)**/**Disable (désactiver)** de la fonctionnalité Cisco Success Network pour modifier le paramètre en conséquence.

Vous pouvez cliquer sur le lien de **sample data (l'exemple de données)** pour voir le type d'informations envoyées à Cisco.

Lorsque vous activez la connexion, lisez la divulgation et cliquez sur **Accep (accepter)**.

Envoi d'événements à Cisco Cloud

Vous pouvez envoyer des événements au serveur Cisco Cloud. À partir de là, divers services de Cisco Cloud peuvent accéder aux événements. Vous pouvez ensuite utiliser ces applications en nuage pour analyser les événements et évaluer les menaces que l'appareil pourrait avoir rencontrées.

Les outils en nuage déterminent si les événements que vous envoyez sont utilisés. Consultez la documentation de l'outil ou examinez les données d'événements pour vous assurer que vous n'envoyez pas d'événements inutilisés vers Cisco Cloud, ce qui gaspillerait votre bande passante et votre espace de stockage. Gardez à l'esprit que les outils tirent les événements de la même source, de sorte que votre sélection doit refléter tous les outils que vous utilisez, pas seulement l'outil le plus restrictif. Par exemple :

- L'outil Security Analytics and Logging (analyse et journalisation de la sécurité) dans Contrôle de Security Cloud peut utiliser tous les événements de connexion.
- Threat Response utilise uniquement des événements de connexion de haute priorité, il n'est donc pas nécessaire d'envoyer tous les événements de connexion au nuage. En outre, il utilisera uniquement les événements hautement prioritaires des informations de sécurité.

Avant de commencer

Vous devez inscrire l'appareil à Cisco Cloud avant de pouvoir activer ce service.

Vous pouvez vous connecter à https://visibility.amp.cisco.com/ dans la région des États-Unis , https://visibility.eu.amp.cisco.com dans la région de l'UE. Vous pouvez regarder des vidéos sur l'utilisation et les avantages de l'application sur YouTube à http://cs.co/CTRvideos. Pour en savoir plus, consultez le *Guide d'intégration Cisco Secure Firewall Threat Defense et SecureX*, que vous pouvez trouver à

https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html.

Procédure

Étape 1 Cliquez **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Cisco Cloud Services**.

Si vous êtes déjà sur la page System Settings (paramètres système), cliquez simplement sur **Cisco Cloud Services** dans la table des matières.

Étape 2 Cliquez sur le contrôle **Enable (activer)**/**Disable (désactiver)** pour l'option **Send Events to the Cisco Cloud (Envoyer les événements vers Cisco Cloud)** afin de modifier le paramètre en conséquence.

Étape 3 Lorsque vous activez le service, vous êtes invité à sélectionner les événements à envoyer au nuage. Vous pouvez modifier ces sélections ultérieurement en cliquant sur **Edit (Modifier)** en regard de la liste des événements sélectionnés. Sélectionnez les types d'événements à envoyer et cliquez sur **OK**.

- **Programme malveillant** : pour toutes les politiques de fichier que vous avez appliquées dans n'importe quelle règle de contrôle d'accès.
- **Intrusion** : pour toutes les politiques d'intrusion que vous avez appliquées dans n'importe quelle règle de contrôle d'accès.
- **Connexion** : pour les règles de contrôle d'accès lorsque vous avez activé la journalisation. Lorsque vous sélectionnez cette option, vous pouvez également choisir d'envoyer tous les événements de connexion ou d'envoyer uniquement les événements de connexion de haute priorité. Les événements de connexion hautement prioritaires sont ceux liés aux connexions qui déclenchent des événements d'intrusion, de fichier ou de programme malveillant, ou qui correspondent aux politiques de blocage des informations de sécurité.

Se désinscrire de Cisco Cloud services

Si vous ne souhaitez plus utiliser les services en nuage, vous pouvez désinscrire l'appareil du nuage. Vous souhaiterez peut-être annuler l'enregistrement lorsque vous retirez le périphérique du service ou que vous l'éliminez de quelque manière que ce soit. Si vous devez modifier la région de vos services en nuage, vous devez vous désinscrire, puis sélectionner la nouvelle région lors de votre réinscription.

La désinscription du nuage à l'aide de cette procédure n'a aucune incidence sur l'inscription de la licence Smart.

Procédure

Étape 1 Cliquez **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Cisco Cloud Services**.

Si vous êtes déjà sur la page System Settings (paramètres système), cliquez simplement sur **Cisco Cloud Services** dans la table des matières.

Étape 2 Sélectionnez **Unregister Cloud Services (annuler l'enregistrement de Cisco Cloud services)** dans la liste déroulante de l'icône en forme d'engrenage ( ).

Étape 3 Lisez l'avertissement et cliquez sur **Unregister (annuler l'inscription)**.

Tous les services en nuage que vous avez activés seront automatiquement désactivés et votre capacité à les réactiver sera supprimée. Cependant, vous verrez maintenant les commandes d'enregistrement dans le nuage et vous pourrez vous inscrire à nouveau.

Activation ou désactivation de l'analyse Web

L'activation de l'analyse Web fournit à Cisco des informations anonymes sur l'utilisation du produit en fonction des pages visitées. Ces renseignements comprennent les pages consultées, le temps passé sur une page, les versions des navigateurs, la version du produit, le nom d'hôte de l'appareil, etc. Ces renseignements peuvent aider Cisco à déterminer les modèles d'utilisation des fonctionnalités et à aider Cisco à améliorer le produit. Toutes les données d'utilisation sont anonymes, et aucune donnée sensible n'est transmise.

L'analyse Web est activée par défaut.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis cliquez sur le lien **System Settings (Paramètres système)** > **Web Analytics (Analyse Web)**.

Si vous êtes déjà dans la page System Settings (Paramètres système), cliquez simplement sur **Web Analytics (Analyse Web)** dans la table des matières.

Étape 2 Cliquez sur le contrôle **Enable**/**Disable** (Activer/Désactiver) de la fonctionnalité **Web Analytics** (Analyse Web) pour modifier le paramètre, au besoin.

Configuration des préférences de filtrage Cloud

Le système obtient la base de données de catégorie URL et de réputation auprès de Cisco Renseignements collectifs sur la sécurité (CSI) (Cisco Talos Intelligence Group (Talos)). Ces préférences contrôlent les mises à jour de la base de données et la façon dont le système gère les URL de catégorie ou de réputation inconnue. Vous devez activer la licence de filtrage d'URL pour définir ces préférences.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis cliquez sur le lien **System Settings (Paramètres système)** > **URL Filtering Preferences (Préférences de filtrage d'URL)**.

Si vous êtes déjà sur la page System Settings (Paramètres système), cliquez simplement sur **URL Filtering Preferences (Préférences de filtrage d'URL)** dans la table des matières.

Étape 2 Configurez les options suivantes :

- **Enable Automatic Updates (Activer les mises à jour automatiques)** : permet au système de vérifier et de télécharger automatiquement les données d'URL mises à jour, qui comprennent les informations de catégorie et de réputation. Le système recherche les mises à jour toutes les 30 minutes, bien que les données soient généralement mises à jour une fois par jour. La valeur par défaut est d'activer les mises à jour. Si vous désélectionnez cette option et que vous utilisez le filtrage de catégorie et de réputation, activez-le périodiquement pour obtenir de nouvelles données URL.
- **Query Cisco CSI for Unknown URLs** (Interroger Cisco CSI pour les URL inconnues) : indique s'il faut vérifier auprès de Cisco CSI pour obtenir des informations mises à jour pour les URL qui n'ont pas de données de catégorie et de réputation dans la base de données locale de filtrage d'URL. Si la recherche renvoie ces informations dans un délai raisonnable, elles sont utilisées lors de la sélection des règles d'accès en fonction des conditions d'URL. Sinon, l'URL correspond à la catégorie Uncategorized (Non classé). La sélection de cette option est importante pour les systèmes bas de gamme, qui installent une base de données d'URL plus petite en raison de contraintes de mémoire.
- **URL Time to Live** (Durée de vie de l'URL) (disponible si vous sélectionnez **Query Cisco CSI for Unknown URLs (Interroger Cisco CSI pour les URL inconnues)**) : durée de mise en cache des valeurs de recherche de catégorie et de réputation pour une URL donnée. À l'expiration de la durée de vie, la prochaine tentative d'accès de l'URL entraîne une nouvelle recherche de catégorie ou de réputation. Un délai plus court permet un filtrage d'URL plus précis, un délai long améliore les performances pour les URL inconnues. Vous pouvez définir le TTL à 2, 4, 8, 12, 24 ou 48 heures, une semaine ou Jamais (par défaut).

Étape 3 Au besoin, vous pouvez **Check the Category (Vérifier la catégorie)** pour une URL.

Vous pouvez vérifier la catégorie et la réputation d'une URL particulière. Saisissez l'URL dans le champ **URL to Check** (URL à vérifier), puis cliquez sur **Go** (Lancer). Vous serez redirigé vers un site Web externe pour consulter les résultats. Si vous êtes en désaccord avec une catégorisation, cliquez sur le lien **Submit a URL Category** Dispute (Soumettre une contestation de catégorie d'URL) et faites-le-nous savoir.

Étape 4 Cliquez sur **Save** (Enregistrer).

Configuration des paramètres de chiffrement TLS/SSL

Les paramètres de chiffrement SSL contrôlent les versions TLS et les suites de chiffrement autorisées pour les connexions TLS/SSL avec le périphérique.

Normalement, la suite de chiffrement que vous configurez devrait avoir plusieurs suites de chiffrement disponibles. Le système déterminera la version TLS la plus élevée prise en charge par le client et le périphérique Firewall Threat Defense, puis choisira une suite de chiffrement prise en charge par les deux et compatible avec la version TLS. Le système sélectionnera la version TLS et la suite de chiffrement les plus puissantes prises en charge par les deux points terminaux pour assurer la connexion la plus sécurisée possible parmi les chiffrements que vous autorisez.

Avant de commencer

Par défaut, le système utilise l'objet DefaultSSLCipher pour définir les suites de chiffrement autorisées. Vous pouvez plutôt choisir l'un des autres objets de chiffrement prédéfinis ou créer votre propre objet personnalisé. Idéalement, créez un seul objet qui inclut toutes les versions et uniquement les chiffrements TLS que vous

souhaitez autoriser. Pour créer votre propre objet, consultez Configurer les objets de chiffrement TLS/SSL, à la page 816.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis sur le lien **System Settings (Paramètres du système)** > **SSL Settings (Paramètres SSL)**.

Étape 2 Configurer les **SSL Settings** (Paramètres SSL)

Ces paramètres contrôlent les chiffrements que les clients sont autorisés à utiliser lors de l'établissement des connexions à distance au réseau privé virtuel.

- **Ciphers** (Chiffrements) : sélectionnez les objets de chiffrement SSL qui définissent les versions TLS et les algorithmes de chiffrement autorisés.

  Cliquez sur **Create New Cipher** (Créer un nouveau chiffrement) au bas de la liste si vous devez créer un objet maintenant.

- **Ephemeral Diffie-Hellman Group Groupe Diffie-Hellman éphémère)** : le groupe DH à utiliser pour les algorithmes de chiffrement éphémères. Pour obtenir une explication des groupes DH, consultez Choix du groupe de module Diffie-Hellman à utiliser, à la page 662. La valeur par défaut est 14.

- **Elliptical Curve DH Grou**p (Groupe DH de courbe elliptique) : le groupe DH à utiliser pour les algorithmes de chiffrement de courbe elliptique. Par défaut, c'est 19.

Étape 3 Cliquez sur **Save** (Enregistrer).

Configurer les objets de chiffrement TLS/SSL

Les objets de chiffrement SSL définissent une combinaison de niveau de sécurité, de versions de protocole TLS/DTLS et d'algorithmes de chiffrement qui peuvent être utilisés lors de l'établissement d'une connexion SSL avec un périphérique Firewall Threat Defense. Utilisez ces objets dans **Device (Périphérique)** > **System Settings (Paramètres système)** > **SSL Settings (Paramètres SSL)** pour définir les exigences de sécurité pour les utilisateurs qui établissent des connexions SSL avec le boîtier.

Les versions TLS et les chiffrements que vous pouvez sélectionner sont contrôlés par votre compte de licence Smart. Si vous respectez les exigences de conformité en matière d'exportation, vous pouvez sélectionner n'importe quelle combinaison d'options. Si votre licence n'est pas conforme à la norme d'exportation, vous êtes limité à TLSv1.0 et DES-DC-SHA, qui sont les options de sécurité les plus basses. Le mode d'évaluation est considéré comme un mode non conforme, de sorte que vos options sont limitées jusqu'à ce que vous obteniez une licence pour le système.

Le système comprend plusieurs objets prédéfinis. Vous ne devez créer de nouveaux objets que si les objets prédéfinis ne correspondent pas à vos exigences de sécurité. Les objets sont les suivants :

- DefaultSSLCipher : il s'agit d'un groupe de niveau de sécurité faible. Il s'agit du réglage par défaut utilisé dans les paramètres SSL pour s'assurer que le plus grand nombre de clients possible puisse effectuer les connexions au système. Il comprend toutes les versions de protocole et tous les chiffrements pris en charge par le système.

- CiscoRecommendedCipher : il s'agit d'un groupe de niveau de sécurité élevé, qui comprend uniquement les chiffrements les plus sécurisés et la version TLS. Ce groupe offre la sécurité la plus élevée, mais vous devez vous assurer que vos clients peuvent utiliser les chiffrements correspondants. Il est plus probable que certains clients ne soient pas en mesure d'établir les connexions en raison de problèmes de non-concordance de chiffrement.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **SSL Ciphers** (Chiffrements SSL) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet (sous **Name**) et, facultativement, une description.

Étape 4 Configurez les options suivantes :

- **Security Level** (Niveau de sécurité) : le niveau de sécurité relatif de l'objet. Notez que si vous modifiez les versions de protocole ou la liste des suites de chiffrement après avoir sélectionné un niveau de sécurité, le niveau réel de sécurité fourni par l'objet peut ne pas correspondre au niveau de sécurité. Effectuez l'une des opérations suivantes :
  - **All** (Tout) : inclut tous les niveaux TLS et toutes les suites de chiffrement dans l'objet, de sécurité faible à sécurité élevée.
  - **Low (Faible)** : comprend toutes les versions et chiffrements TLS, ce qui permet aux utilisateurs d'établir des connexions avec les chiffrements les moins sécurisés. Pour une licence non conforme à l'exportation, cela inclut TLSv1.0 et DES-CBC-SHA.
  - **Medium** (Moyen) : comprend toutes les versions TLS, mais supprime certains chiffrements plutôt non sécurisés. Il n'y a qu'une différence minimale entre cette option et l'option Faible/Tout. Vous ne pouvez pas utiliser cette option avec les licences qui ne sont pas conformes à l'exportation.
  - **High** (Élevé) : autorise uniquement les dernières versions DTLS et TLS, et les chiffrements qui fonctionnent avec ces versions. Cette option limite les connexions aux chiffrements les plus sécurisés actuellement disponibles. Vous ne pouvez pas utiliser cette option avec les licences qui ne sont pas conformes à l'exportation.
  - **Custom** (Personnalisé) : sélectionnez cette option si vous souhaitez sélectionner les versions TLS et les chiffrements individuellement. Les options que vous sélectionnez détermineront si vous définissez un paramètre de chiffrement de sécurité élevée ou faible. Bien qu'il n'y ait pas de valeurs par défaut pour un objet personnalisé, si vous avez sélectionné un autre niveau avant de sélectionner personnalisé, les options affichées précédemment restent sélectionnées pour votre commodité.
- **Protocol Versions** (Versions de protocole) : versions TLS/DTLS qu'un client est autorisé à utiliser lors de l'établissement d'une connexion TLS/SSL avec le périphérique Firewall Threat Defense. Pour un objet personnalisé, sélectionnez les versions que vous souhaitez prendre en charge. Pour les autres niveaux

de sécurité, il ne faut généralement pas modifier la liste, mais vous pouvez ajouter ou supprimer des versions comme vous le souhaitez.

- **Applicable Cipher Suites** (Suites de chiffrement applicables) : les algorithmes de chiffrement que le client peut utiliser. Cliquez sur **+** pour ajouter de nouvelles suites; cliquez sur **x** dans une suite pour la supprimer.

  Votre sélection de version de protocole contrôle les suites disponibles dans cette liste. Si vous modifiez les versions de protocole, toute suite sélectionnée qui ne fonctionne plus avec les versions sélectionnées est signalée : vous devez les supprimer ou rajouter la version de protocole requise.

Étape 5 Cliquez sur **OK**.



CHAPITRE 27

Gestion du système

Les rubriques suivantes expliquent comment effectuer les tâches de gestion du système telles que la mise à jour des bases de données du système ainsi que la sauvegarde et la restauration du système.

- Installation des mises à jour logicielles, à la page 819
- Sauvegarde et restauration du système, à la page 830
- Audit et gestion du changement, à la page 836
- Exporter la configuration du périphérique., à la page 843
- Gestion du Gestionnaire de périphériques de pare-feu et accès des utilisateurs Firewall Threat Defense, à la page 843
- Redémarrage ou arrêt du système, à la page 850
- Dépannage du système, à la page 851
- Basculement entre la gestion locale et la gestion à distance, à la page 864
- Tâches de gestion du matériel, à la page 867

Installation des mises à jour logicielles

Vous pouvez installer les mises à jour des bases de données du système et du logiciel système. Les rubriques suivantes expliquent comment installer ces mises à jour.

Mise à jour des bases de données système et des flux

Le système utilise plusieurs bases de données et flux de Security Intelligence pour fournir des services avancés. Cisco fournit des mises à jour de ces bases de données et de ces flux afin que vos politiques de sécurité utilisent les dernières informations disponibles.

Aperçu des mises à jour de la base de données du système et des flux

Firewall Threat Defense utilise les bases de données et les flux suivants pour fournir des services avancés.

Règles d'intrusion

À mesure que de nouvelles vulnérabilités sont découvertes, Cisco Talos Intelligence Group (Talos) publie des mises à jour de règles de prévention des intrusions que vous pouvez importer. Ces mises à jour affectent les règles de prévention des intrusions, les règles de préprocesseur et les politiques qui utilisent les règles.

Les mises à jour des règles de prévention des intrusions fournissent des règles de prévention des intrusions et des règles de préprocesseur nouvelles et mises à jour, des états modifiés pour les règles existantes et des paramètres de politique de prévention des intrusions par défaut modifiés. Les mises à jour de règles peuvent également supprimer des règles, fournir de nouvelles catégories de règles et variables par défaut, et modifier les valeurs des variables par défaut.

Pour que les modifications apportées par une mise à jour de règles de prévention des intrusions prennent effet, vous devez redéployer les configurations.

Les mises à jour de règles peuvent être volumineuses; importez-les pendant les périodes de faible utilisation du réseau. Sur les réseaux lents, une tentative de mise à jour peut échouer et vous devrez réessayer.

Base de données de géolocalisation (GeoDB)

La base de données de géolocalisation Cisco (GeoDB) est une base de données de données géographiques (pays, ville, coordonnées, etc.) associées à des adresses IP routables.

Les mises à jour de GeoDB fournissent des renseignements à jour sur les emplacements physiques que votre système peut associer aux adresses IP routables détectées. Vous pouvez utiliser les données de géolocalisation comme condition dans les règles de contrôle d'accès.

Le temps nécessaire pour mettre à jour la base de données GeoDB dépend de votre appareil ; l'installation prend habituellement entre 30 et 40 minutes. Bien qu'une mise à jour de GeoDB n'interrompe aucune autre fonction du système (y compris la collecte continue d'informations de géolocalisation), la mise à jour consomme des ressources système pendant qu'elle se termine. Tenez compte de ces éléments lors de la planification de vos mises à jour.

Base de données relative aux vulnérabilités (VDB)

La base de données sur les vulnérabilités de Cisco (VDB) est une base de données des vulnérabilités connues auxquelles les hôtes peuvent être exposés, ainsi que des empreintes pour les systèmes d'exploitation, les clients et les applications. Le système de pare-feu corrèle ces empreintes avec les vulnérabilités pour vous aider à déterminer si un hôte particulier augmente le risque de compromission du réseau. CiscoCisco Talos Intelligence Group (Talos)publie des mises à jour périodiques de la VDB.

Le temps nécessaire pour mettre à jour la VDB et ses mappages des vulnérabilités dépend du nombre d'hôtes dans votre cartographie du réseau. Vous pouvez planifier la mise à jour pendant les périodes de faible utilisation du système afin de minimiser l'impact de tout temps d'arrêt. En règle générale, divisez le nombre d'hôtes de votre réseau par 1 000 pour déterminer le nombre approximatif de minutes nécessaires pour effectuer la mise à jour.

Après avoir mis à jour la VDB, vous devez redéployer les configurations pour que les détecteurs d'applications et les empreintes de systèmes d'exploitation mis à jour prennent effet.

Flux de renseignements sur la sécuritéCisco Talos Intelligence Group (Talos)

Talos donne accès à des flux de renseignements régulièrement mis à jour à utiliser dans les politiques de Security Intelligence. Les sites qui représentent des menaces de sécurité, comme les programmes malveillants, les pourriels, les réseaux de zombies et l'hameçonnage peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer des configurations personnalisées. Ces flux contiennent des adresses et des URL pour les menaces connues. Lorsque le système met à jour un flux, il n'est pas nécessaire de le redéployer. Les nouvelles listes sont utilisées pour évaluer les connexions ultérieures.

Base de données de catégorie/réputation d'URL

Le système obtient la base de données de catégorie URL et de réputation auprès de Cisco Collective Security Intelligence (CSI). Si vous configurez des règles de contrôle d'accès avec filtrage d'URL sur

la base de la catégorie et de la réputation, les URL demandées sont comparées à cette base de données. Vous pouvez configurer les mises à jour de base de données et d'autres préférences de filtrage d'URL dans **System Settings (Paramètres du système)** > **URL Filtering Preferences (Préférences de filtrage d'URL)**. Vous ne pouvez pas gérer les mises à jour de la base de données de catégorie/réputation d'URL de la même manière que les mises à jour des autres bases de données du système.

Mise à jour des bases de données du système.

Vous pouvez récupérer manuellement et appliquer les mises à jour de la base de données du système selon votre commodité. Les mises à jour sont récupérées à partir du site d'assistance de Cisco. Ainsi, il doit y avoir un chemin d'accès à l'Internet à partir de l'adresse de gestion du système.

Sinon, vous pouvez récupérer vous-même les paquets de mise à jour sur Internet, puis les charger à partir de votre ordinateur. Cette méthode est principalement destinée aux réseaux isolés, où il n'y a pas de chemin d'accès à Internet pour récupérer les mises à jour de Cisco. Téléchargez les mises à jour à partir de software.cisco.com à partir des mêmes dossiers où vous téléchargeriez les mises à niveau logicielles système.



Remarque En mai 2022, nous avons scindé la base de données GeoDB en deux ensembles : un ensemble de codes de pays qui mappe les adresses IP aux pays/continents, et un ensemble d'adresses IP qui contient des données contextuelles supplémentaires associées aux adresses IP routables. Le Gestionnaire de périphériques de pare-feu n'a pas utilisé et n'a jamais utilisé les informations contenues dans le paquet IP. Cette séparation permet d'économiser beaucoup d'espace disque dans les déploiements Firewall Threat Defense gérés localement. Si vous obtenez vous-même la base de données GeoDB de Cisco, assurez-vous d'obtenir le paquet du code de pays, qui porte le même nom de fichier que l'ancien paquet tout-en-un : Cisco_GEODB_Update-*date-build*.

Vous pouvez également configurer un calendrier régulier pour récupérer et appliquer les mises à jour de la base de données. Étant donné que ces mises à jour peuvent être volumineuses, planifiez-les pour les périodes de faible activité du réseau.



Remarque Lorsqu'une mise à jour d'une base de données est en cours, vous pourriez trouver que l'interface utilisateur est lente pour répondre à vos actions.

Avant de commencer

Pour éviter toute incidence potentielle sur les modifications en attente, déployez la configuration sur le périphérique avant de mettre à jour manuellement ces bases de données.

Sachez que les mises à jour de VDB et de catégories d'URL peuvent supprimer des applications ou des catégories. Vous devez mettre à jour toutes les règles de contrôle d'accès ou de déchiffrement SSL qui utilisent ces éléments obsolètes avant de pouvoir déployer les modifications.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis cliquez sur **View Configuration** (Afficher la configuration) dans le résumé des mises à jour.

Cela ouvre la page Updates (Mises à jour). Les renseignements sur la page affichent la version actuelle de chaque base de données ainsi que la date et l'heure de la dernière mise à jour de chaque base de données.

Étape 2 Pour mettre à jour manuellement une base de données, cliquez sur l'une des options suivantes dans la section de cette base de données :

- **Update from Cloud** (Mettre à jour à partir du cloud) : pour que Gestionnaire de périphériques de pare-feu récupère le package de mise à jour auprès de Cisco. Il s'agit de la méthode la plus simple et de la plus fiable, mais il doit y avoir un chemin d'accès à Internet pour l'utiliser.
- **(flèche vers le bas)** > ***option*** : pour sélectionner le package de mise à jour à partir de votre poste de travail ou d'un lecteur connecté à votre poste de travail. L'option sera l'une des suivantes :
  - **Select File** (Sélectionner un fichier) : sélectionnez un ensemble VDB ou de géolocalisation. Vous devez sélectionner une version plus récente que celle installée. Vous ne pouvez pas rétrograder ces paquets.
  - **Update to Newer Version** (Mettre à jour vers une version plus récente) : sélectionnez un ensemble de règles de prévention des intrusions qui est plus récent que celui actuellement installé.
  - **Downgrade to Older Version** (Rétrograder à une version antérieure) : sélectionnez un ensemble de règles de prévention des intrusions plus ancien que celui actuellement installé.

Les mises à jour de règles et de VDB nécessitent un déploiement de configuration pour les rendre actives. Lorsque vous effectuez une mise à jour à partir du Cloud, il vous est demandé si vous souhaitez procéder au déploiement maintenant ; cliquez sur **Yes** (Oui). Si vous cliquez sur **No** (Non), n'oubliez pas de lancer une tâche de déploiement dès que vous le pouvez.

Si vous chargez votre propre fichier, vous devez toujours déployer les modifications manuellement.

Remarque
Lors du chargement manuel d'un ensemble de règles de prévention des intrusions, assurez-vous de charger le type de package approprié pour votre version Snort, SRU pour Snort 2, LSP pour Snort 3. Vous pouvez charger un package pour la version Snort non active, mais elle ne sera activée que si vous changez de version. Pour en savoir plus sur le changement de version de Snort, consultez Commutation entre Snort 2 et Snort 3, à la page 546.

Étape 3 (Facultatif) Pour configurer une planification de mise à jour régulière de la base de données :

a) Cliquez sur le lien **Configure** (Configurer) dans la section de la base de données souhaitée. S'il existe déjà un calendrier, cliquez sur **Edit** (Modifier).

Les calendriers de mise à jour des bases de données sont distincts. Vous devez définir les planifications séparément.

b) Spécifiez l'heure de début de la mise à jour :

- La fréquence de la mise à jour (quotidienne, hebdomadaire ou mensuelle).
- Pour les mises à jour hebdomadaires ou mensuelles, les jours de la semaine ou du mois pendant lesquels vous souhaitez que la mise à jour se produise.
- L'heure à laquelle vous souhaitez que la mise à jour commence. L'heure que vous précisez est ajustée selon l'heure avancée. Elle sera reculée ou avancée à chaque changement d'heure dans votre région. Vous devez modifier le calendrier au moment du changement d'heure si vous souhaitez conserver cette heure tout au long de l'année.

c) Pour les mises à jour de règles ou de VDB, cochez la case **Automatically Deploy the Update** (déployer automatiquement la mise à jour) si vous souhaitez que le système déploie la configuration chaque fois que la base de données est mise à jour.

La mise à jour n'est effective que lorsqu'elle est déployée. Le déploiement automatique déploie également toutes les autres modifications de configuration qui ne sont pas encore déployées.

d) Cliquez sur **Save** (enregistrer).

Remarque
Si vous souhaitez supprimer une planification récurrente, cliquez sur le lien **Edit** (Modifier) pour ouvrir la boîte de dialogue de planification, puis cliquez sur le bouton **Remove** (Supprimer).

Mise à jour des flux de renseignements de sécurité

Cisco Talos Intelligence Group (Talos) fournit un accès à des flux de renseignements de sécurité régulièrement mis à jour. Les sites qui représentent des menaces de sécurité, comme les programmes malveillants, les pourriels, les réseaux de zombies et l'hameçonnage peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer des configurations personnalisées. Lorsque le système met à jour un flux, il n'est pas nécessaire de le redéployer. Les nouvelles listes sont utilisées pour évaluer les connexions ultérieures.

Si vous souhaitez contrôler strictement quand le système met à jour un flux à partir d'Internet, vous pouvez désactiver les mises à jour automatiques pour ce flux. Cependant, les mises à jour automatiques assurent l'obtention des données pertinentes les plus à jour.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis cliquez sur **View Configuration (Afficher la configuration)** dans le résumé Updates (Mises à jour).

Cela ouvre la page Updates (Mises à jour). Les renseignements sur la page affichent la version actuelle des **Security Intelligence Feeds** (Flux de renseignements de sécurité) ainsi que la date et l'heure de la dernière mise à jour des flux.

Étape 2 Pour mettre à jour manuellement les flux, cliquez sur **Update Now** (Mettre à jour maintenant) dans le groupe **Security Intelligence Feeds (Flux de renseignements de sécurité)**.

Si vous mettez à jour manuellement les flux sur une unité dans un groupe à haute disponibilité, vous devez également les mettre à jour manuellement sur l'autre unité pour assurer la cohérence.

Étape 3 (Facultatif) Pour configurer une fréquence de mise à jour régulière :

a) Cliquez sur le lien **Configure** (Configurer) dans la section des flux Cisco. S'il existe déjà un calendrier, cliquez sur **Edit** (Modifier).

b) Sélectionnez la fréquence de mise à jour souhaitée.

La valeur par défaut est **Hourly (Toutes les heures)**. Vous pouvez également définir une mise à jour **Daily (Journalière)** (précisez l'heure du jour) ou une mise à jour **Weekly** (Hebdomadaire) (sélectionnez les jours de la semaine et l'heure du jour). L'heure que vous précisez est ajustée selon l'heure avancée. Elle sera reculée ou avancée à chaque changement d'heure dans votre région. Vous devez modifier le calendrier au moment du changement d'heure si vous souhaitez conserver cette heure tout au long de l'année.

Cliquez sur **Delete** (Supprimer) pour empêcher les mises à jour automatiques.

c) Cliquez sur **OK**.

Mise à niveau Firewall Threat Defense

Utilisez cette procédure pour mettre à niveau un périphérique autonome Firewall Threat Defense. Si vous devez mettre à jour FXOS, faites-le en premier. Pour mettre à niveau la défense contre les menaces haute disponibilité, voir Mise à niveau de la haute disponibilité Firewall Threat Defense, à la page 236.

Mise en garde Le trafic est abandonné pendant la mise à niveau. Même si le système semble inactif ou ne répond pas, ne le redémarrez pas ou ne l'éteignez pas manuellement pendant la mise à niveau. vous pourriez rendre le système inutilisé et nécessiter une réinitialisation. Vous pouvez annuler manuellement les mises à niveau majeures ou de maintenance en cours ou qui ont échoué, et réessayer les mises à niveau qui ont échoué. Si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Pour en savoir plus sur ces problèmes et d'autres que vous pouvez rencontrer pendant la mise à niveau, consultez Dépannage des mises à niveau de la protection contre les menaces, à la page 828.

Avant de commencer

Terminer la planification de la mise à niveau. Vérifiez que votre déploiement est intègre et communique correctement.

Astuces La planification de la mise à niveau commence par la lecture du Notes de version de Secure Firewall Threat Defense. Elle inclut ensuite la création de sauvegardes, l'obtention des paquets de mise à niveau et l'exécution des mises à niveau associées (comme FXOS pour Firepower 4100/9300). Elle comprend également la vérification des modifications de configuration nécessaires, de la préparation, de la vérification de l'espace disque et de la vérification des tâches en cours d'exécution et planifiées. Pour en savoir plus, consultez le informations sur la planification de la mise à niveau dans le Guide de mise à niveau de Cisco Firepower Threat Defense pour Firepower Device Manager, version 7.1.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le volet des mises à jour (Updates).
Le volet de mise à niveau du système indique la version du logiciel en cours d'exécution et tout paquet de mise à niveau que vous avez déjà téléversé.

Étape 2 Téléverser le paquet de mise à niveau

Vous ne pouvez téléverser qu'un seul paquet. Si vous téléversez un nouveau fichier, il remplace l'ancien fichier. Assurez-vous que le paquet convient à votre version cible et au modèle de périphérique. Cliquez sur **Parcourir** ou sur **Remplacer le fichier** pour commencer le téléversement.

Une fois le téléversement terminé, le système affiche une boîte de dialogue de confirmation. Avant de cliquer sur **OK**, sélectionnez éventuellement **Exécuter la mise à niveau Immédiatement** pour et choisissez les options de restauration et la mise à niveau maintenant. Si vous effectuez une mise à niveau maintenant, il est particulièrement important d'avoir complété autant que possible la liste de contrôles avant mise à niveau (voir l'étape suivante).

Étape 3 Effectuer les vérifications finales préalables à la mise à niveau, y compris la vérification de l'état de préparation.

Consultez la liste de contrôles avant mise à niveau. Assurez-vous d'avoir effectué toutes les tâches pertinentes, en particulier les vérifications finales. Si vous n'exécutez pas la vérification de la préparation manuellement, elle s'exécute lorsque vous lancez la mise à niveau. Si la vérification échoue, la mise à niveau est annulée. Pour en savoir plus, consultez Exécution d'une vérification de l'état de préparation aux mises à niveau, à la page 825.

Étape 4 Cliquez sur **Upgrade Now** (Installer > Mettre à niveau maintenant) pour lancer le processus d'installation de la mise à niveau.

a) Choisissez les options de restauration.

Vous pouvez **Annuler automatiquement en cas d'échec de la mise à niveau et revenir à la version précédente**. Lorsque cette option est activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci qu'elle soit majeure ou de maintenance. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué.

b) Cliquez sur **Continuer** pour mettre à niveau et redémarrer le périphérique.

Vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la mise à niveau jusqu'à ce que le périphérique redémarre. La page comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, vous pouvez annuler manuellement ou tenter de nouveau la mise à niveau.

Le trafic est abandonné pendant la mise à niveau. Pour ISA 3000 uniquement, si vous avez configuré le contournement matériel pour une panne de courant, le trafic est abandonné pendant la mise à niveau, mais transmis sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.

Étape 5 Reconnectez-vous quand vous le pouvez et vérifiez la réussite de la mise à niveau.

La page Device Summary (sommaire du périphérique) affiche la version du logiciel actuellement exécutée.

Étape 6 Effectuer les tâches postérieures à la mise à niveau.

a) Mettez à jour les bases de données du système. Si les mises à jour automatiques ne sont pas configurées pour les règles de prévention des intrusions, VDB et GeoDB, mettez-les à jour maintenant.
b) Apportez toutes les modifications de configuration requises après la mise à niveau.
c) Déployez.

Exécution d'une vérification de l'état de préparation aux mises à niveau

Avant d'installer une mise à niveau, le système exécute une vérification de préparation pour s'assurer que la mise à niveau est valide pour le système et pour examiner les autres facteurs qui peuvent empêcher la réussite de la mise à niveau. Si la vérification de préparation échoue, vous devez résoudre les problèmes avant de relancer l'installation. Si la vérification a échoué, vous serez informé de l'échec la prochaine fois que vous tenterez l'installation, et vous aurez la possibilité de forcer l'installation si vous le souhaitez.

Vous pouvez également exécuter manuellement le test de préparation avant de lancer la mise à niveau, comme le décrit cette procédure.

Avant de commencer

Chargez l'ensemble de mises à niveau que vous souhaitez vérifier.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le résumé des mises à jour (Updates).

La section **System Upgrade** (mise à niveau du système) affiche la version du logiciel en cours d'exécution et toute mise à jour que vous avez déjà téléchargée.

Étape 2 Consultez la section **Readiness Check** (vérification de l'état de préparation).

- Si la vérification de mise à niveau n'a pas encore été effectuée, cliquez sur le lien **Run Upgrade Readiness Check** (exécuter la vérification de l'état préparation aux mises à niveau). La progression de la vérification s'affiche dans cette zone. Le processus devrait prendre environ 20 secondes.
- Si la vérification de mise à niveau a déjà été exécutée, cette section indique si la vérification s'est soldée par une réussite ou un échec. En cas d'échec, cliquez sur **See Details** pour consulter plus d'information au sujet de la vérification de l'état de préparation. Après avoir résolu les problèmes, relancez la vérification.

Étape 3 Si la vérification de l'état de préparation conduit à un échec, vous devez résoudre les problèmes avant d'installer la mise à niveau. Les informations détaillées comprennent de l'aide pour résoudre les problèmes signalés. À la suite d'un script d'échec, cliquez sur le lien **Show Recovery Message** pour afficher les informations.

Voici quelques problème courants :

- Incompatibilité de la version de FXOS - Sur les systèmes où vous installez les mises à niveau de FXOS séparément, comme le Firepower 4100/9300, un paquet de mise à niveau peut nécessiter une version minimale de FXOS différente de la version du logiciel Firewall Threat Defense que vous exécutez actuellement. Dans ce cas, vous devez d'abord mettre à niveau FXOS avant de pouvoir mettre à niveau le logiciel Firewall Threat Defense.
- Modèle de périphérique non pris en charge : l'ensemble de mise à niveau ne peut pas être installé sur ce périphérique. Vous avez peut-être téléchargé le mauvais paquet, ou l'appareil est un ancien modèle qui n'est tout simplement plus pris en charge par la nouvelle version du logiciel Firewall Threat Defense. Veuillez vérifier la compatibilité de l'appareil et télécharger un ensemble pris en charge, s'il en existe un.
- Espace disque insuffisant : Si l'espace disponible est insuffisant, essayez de supprimer les fichiers inutiles, comme les sauvegardes du système. Supprimez uniquement les fichiers que vous avez créés.

Surveillance des mises à niveau de Firewall Threat Defense

Lorsque vous lancez la mise à niveau de Firewall Threat Defense, vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la progression globale de la mise à niveau. La page

comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, la page vous permet d'annuler manuellement ou de tenter de nouveau la mise à niveau.

Vous pouvez également vous connecter en SSH au périphérique et utiliser l'interface de ligne de commande : **show upgrade status**. Ajoutez le mot-clé **continuous** pour afficher les entrées de journal telles qu'elles sont créées et **detail** pour afficher des informations détaillées. Ajoutez les deux mots-clés pour obtenir des informations détaillées en continu.

Une fois la mise à niveau terminée, vous perdez l'accès à la page d'état et à l'interface de ligne de commande lorsque le périphérique redémarre.

Annulation ou nouvelle tentative des Firewall Threat Defense mises à niveau

Utilisez la page d'état de la mise à niveau ou l'interface de ligne de commande pour annuler manuellement les mises à niveau majeures ou de maintenance qui ont échoué ou en cours, et pour réessayer les mises à niveau qui ont échoué :

- Page d'état de mise à niveau : cliquez sur **Annuler la mise à niveau** pour annuler une mise à niveau en cours. Si la mise à niveau échoue, vous pouvez cliquer sur **Annuler la mise à niveau** pour arrêter la tâche et revenir à l'état du périphérique avant la mise à niveau, ou cliquer sur **Continuer** pour réessayer la mise à niveau.
- CLI : Utilisez la commande **upgrade cancel** pour annuler une mise à niveau en cours. Si la mise à niveau échoue, vous pouvez utiliser **upgrade cancel** pour arrêter la tâche et revenir à l'état du périphérique avant la mise à niveau, ou utiliser **upgrade retry** pour réessayer la mise à niveau.



Remarque Par défaut, Firewall Threat Defense revient automatiquement à son état d'avant la mise à niveau en cas d'échec de cette dernière (« auto-cancel ») (Annulation automatique). Pour pouvoir annuler manuellement ou réessayer une mise à niveau ayant échoué, désactivez l'option d'annulation automatique lorsque vous lancez la mise à niveau. Dans un déploiement à haute disponibilité, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli.

L'annulation et la nouvelle tentative ne sont pas prises en charge pour les correctifs. Pour en savoir plus sur la reprise d'une mise à niveau réussie, consultez Rétablissement Firewall Threat Defense en cours..., à la page 827.

Rétablissement Firewall Threat Defense en cours...

Si une mise à niveau majeure ou de maintenance réussit, mais que le système ne fonctionne pas comme prévu, vous pouvez revenir en arrière. Le rétablissement de Firewall Threat Defense ramène le logiciel à l'état qu'il avait avant la dernière mise à niveau majeure ou de maintenance; les modifications de configuration ultérieures à la mise à niveau ne sont pas conservées. Le rétablissement après l'application d'un correctif supprime également les correctifs. Notez que vous ne pouvez pas annuler des correctifs ou des correctifs rapides individuels.

La procédure suivante explique comment restaurer à partir de Gestionnaire de périphériques de pare-feu. Si vous ne pouvez pas accéder à Gestionnaire de périphériques de pare-feu, vous pouvez revenir à la ligne de

commande Firewall Threat Defense dans une session SSH en utilisant la commande **upgrade revert**. Vous pouvez utiliser la commande **show upgrade revert-info** pour voir à quelle version le système retournera.

Avant de commencer

Si l'unité fait partie d'une paire à haute disponibilité, vous devez rétablir les deux unités. Idéalement, lancez la restauration sur les deux unités en même temps afin que la configuration puisse être restaurée sans problème de basculement. Ouvrez des sessions avec les deux unités et vérifiez que le rétablissement est possible sur chacune, puis démarrez les processus. Notez que le trafic sera interrompu pendant la restauration, donc effectuez-la si possible en dehors des heures ouvrables.

Pour les châssis Firepower 4100/9300, les versions principales Firewall Threat Defense ont une version FXOS associée spécialement qualifiée et recommandée. Cela signifie qu'après avoir rétabli le logiciel Firewall Threat Defense, vous exécutez peut-être une version non recommandée de FXOS (trop récente). Bien que les nouvelles versions de FXOS soient rétrocompatibles avec les anciennes versions de Firewall Threat Defense, nous effectuons des tests avancés des combinaisons recommandées. Vous ne pouvez pas passer à une version antérieure de FXOS, donc si vous vous trouvez dans cette situation et que vous souhaitez exécuter une combinaison recommandée, vous devrez recréer l'image du périphérique.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le résumé des mises à jour **(Updates)**.

Étape 2 Dans la section **System Upgrade** (mise à niveau du système), cliquez sur le lien **Revert Upgrade** (annuler la mise à niveau).

Une boîte de dialogue de confirmation s'affiche et affiche la version actuelle et la version à laquelle le système sera restauré. Si aucune version n'est disponible pour la restauration, il n'y a pas de lien **Annuler la mise à niveau**.

Étape 3 Si la version cible vous convient (et qu'une version est disponible), cliquez sur **Revert** (Restaurer).

Après avoir effectué le retour en arrière, vous devez réenregistrer le périphérique auprès du Smart Software Manager.

Dépannage des mises à niveau de la protection contre les menaces

Ces problèmes peuvent se produire lorsque vous mettez à niveau un périphérique, qu'il soit autonome ou au sein d'une paire à haute disponibilité. Pour résoudre les problèmes spécifiques aux mises à niveau à haute disponibilité, consultez Dépannage des mises à niveau de Threat Defense haute disponibilité, à la page 238.

Erreurs relatives au paquet de mise à niveau

Pour trouver le bon paquet de mise à niveau, sélectionnez ou recherchez votre modèle sur Site d'assistance et de téléchargement Cisco, puis accédez à la page de téléchargement du logiciel pour la version appropriée. Les paquets de mise à niveau disponibles sont répertoriés avec les paquets d'installation, les correctifs rapides et les autres téléchargements applicables. Les noms des fichiers de paquet de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif), la version du logiciel et la version.

Les paquets de mise à niveau à partir de la version 6.2.1+ sont signés et se terminent par .sh.REL.tar. Ne décompressez pas les paquets de mise à niveau signés. Ne renommez pas les paquets de mise à niveau et ne les transférez pas par courriel.

Impossible d'atteindre le périphérique pendant la mise à niveau.

Les périphériques arrêtent de transmettre le trafic pendant la mise à niveau ou en cas d'échec de la mise à niveau. Avant d'effectuer la mise à niveau, assurez-vous que le trafic en provenance de votre emplacement n'a pas à traverser le périphérique lui-même pour accéder à l'interface de gestion du périphérique .

Le périphérique semble inactif ou ne répond pas pendant la mise à niveau.

Vous pouvez annuler manuellement les mises à niveau majeures et de maintenance en cours; voir Annulation ou nouvelle tentative des Firewall Threat Defense mises à niveau, à la page 827. Si le périphérique ne répond pas ou si vous ne pouvez pas annuler la mise à niveau, communiquez avec Centre d'assistance technique Cisco (TAC).



Mise en garde Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez *pas* manuellement pendant la mise à niveau. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image.

La mise à niveau a réussi, mais le système ne fonctionne pas comme vous le souhaitez.

Tout d'abord, assurez-vous que les informations en cache sont actualisées. N'actualisez pas simplement la fenêtre du navigateur pour vous reconnecter. Supprimez plutôt tout chemin « supplémentaire » de l'URL et reconnectez-vous à la page d'accueil; par exemple, http://threat-defense.exemple.com/.

Si vous continuez à rencontrer des problèmes et que vous devez revenir à une version majeure ou de maintenance antérieure, vous pourrez peut-être revenir à une version majeure ou de maintenance antérieure; voir Rétablissement Firewall Threat Defense en cours..., à la page 827. Si vous ne pouvez pas revenir en arrière, vous devez recréer l'image.

Échec de la mise à niveau.

Lorsque vous lancez une mise à niveau majeure ou de maintenance, utilisez la commande **Annuler automatiquement en cas d'échec de la mise à niveau...** Option d'annulation automatique pour choisir ce qui se passe en cas d'échec de la mise à niveau, comme suit :

- Annulation automatique activée (par défaut) : si la mise à niveau échoue, la mise à niveau est annulée et le périphérique revient automatiquement à l'état qu'il avait avant la mise à niveau. Corrigez les problèmes et réessayez.
- Annulation automatique désactivée : si la mise à niveau échoue, le périphérique reste tel qu'il est. Corrigez les problèmes et réessayez immédiatement, ou annulez manuellement la mise à niveau et réessayez ultérieurement.

Pour en savoir plus, consultez Annulation ou nouvelle tentative des Firewall Threat Defense mises à niveau, à la page 827. Si vous ne pouvez pas réessayer ou annuler, ou si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Recréation d'image du périphérique

La recréation d'image d'un périphérique implique l'effacement de la configuration du périphérique et l'installation d'une nouvelle image logicielle. L'intention de la recréation d'image est d'avoir une installation propre avec une configuration d'usine par défaut.

Vous devriez recréer l'image du périphérique dans les circonstances suivantes :

- Vous souhaitez convertir le système du logiciel ASA au logiciel Firewall Threat Defense. Vous ne pouvez pas mettre à niveau un périphérique exécutant une image ASA vers un périphérique exécutant une image Firewall Threat Defense.
- Le périphérique exécute une image antérieure à la version 6.1.0, et vous souhaitez effectuer une mise à niveau vers la version 6.1 ou une image ultérieure et configurer le périphérique à l'aide de l'option Gestionnaire de périphériques de pare-feu. Vous ne pouvez pas utiliser le Centre de gestion Firepower (FMC) pour mettre à niveau un périphérique antérieur à la version 6.1, puis passer à la gestion locale.
- Le périphérique ne fonctionne pas correctement et toutes les tentatives de correction de la configuration ont échoué.

Pour en savoir plus sur la réinitialisation d'un appareil, consultez *Réinitialiser l'appareil de protection contre les menaces Cisco ASA ou Threat Defense* ou le guide de *démarrage rapide de la défense contre les menaces* pour votre modèle d'appareil. Ces guides sont disponibles sur http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html.

Sauvegarde et restauration du système

Vous pouvez sauvegarder la configuration du système afin de pouvoir restaurer le périphérique si la configuration est corrompue en raison d'une mauvaise configuration ultérieure ou d'un incident physique.

Vous pouvez restaurer une sauvegarde sur un périphérique de remplacement uniquement si les deux périphériques sont du même modèle et exécutent la même version du logiciel (y compris le numéro de build, pas seulement la même version mineure). N'utilisez pas le processus de sauvegarde et de restauration pour copier des configurations entre des périphériques. Un fichier de sauvegarde contient des informations qui identifient de manière unique un périphérique et ne peuvent pas être partagées.



Remarque La sauvegarde n'inclut pas la configuration de l'adresse IP de gestion. Ainsi, lorsque vous récupérez un fichier de sauvegarde, l'adresse de gestion n'est pas remplacée à partir de la copie de sauvegarde. Cela garantit que toutes les modifications que vous avez apportées à l'adresse sont conservées et permet également de restaurer la configuration sur un périphérique différent sur un segment de réseau différent. La sauvegarde ne comprend pas non plus les informations de licence ou d'enregistrement dans le nuage, de sorte que tout état de licence ou d'enregistrement dans le nuage qui existe au moment de la restauration est conservé.

Les sauvegardes comprennent la configuration uniquement, et non le logiciel système. Si vous devez recréer complètement l'image du périphérique, vous devez réinstaller le logiciel, puis vous pouvez charger une sauvegarde et récupérer la configuration.

La base de données de configuration est verrouillée pendant la sauvegarde. Vous ne pouvez pas apporter de modifications à la configuration pendant une sauvegarde, bien que vous puissiez afficher les politiques, les tableaux de bord, etc. Pendant une restauration, le système est complètement indisponible.

Le tableau de la page Backup and Restore (Sauvegarde et restauration) répertorie toutes les copies de sauvegarde existantes qui sont disponibles sur le système, y compris le nom de fichier de la sauvegarde, la date et l'heure de sa création et la taille du fichier. Le type de sauvegarde (manuelle, planifiée ou récurrente) dépend de la façon dont vous avez demandé au système de créer cette copie de sauvegarde.



Astuces Les copies de sauvegarde sont créées sur le système lui-même. Vous devez télécharger manuellement les copies de sauvegarde et les stocker sur des serveurs sécurisés pour vous assurer d'avoir les copies de sauvegarde dont vous avez besoin pour la reprise sur sinistre. Le système conserve jusqu'à 3 copies de sauvegarde sur le périphérique. Les nouvelles sauvegardes remplacent la sauvegarde la plus ancienne.

Les rubriques suivantes expliquent comment gérer les opérations de sauvegarde et de restauration.

Sauvegarder le système immédiatement

Vous pouvez démarrer une sauvegarde quand vous le souhaitez.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuratio**n (Afficher la configuration) dans le résumé Backup and Restore (Sauvegarde et restauration).

Cela ouvre la page Backup and Restore (Sauvegarde et restauration). Le tableau répertorie toutes les copies de sauvegarde existantes qui sont disponibles sur le système.

Étape 2 Cliquez sur **Manual Backup (Sauvegarde manuelle)** > **Back Up Now (Sauvegarder maintenant)**.

Étape 3 Entrez un nom pour la sauvegarde et, facultativement, une description.

Si vous décidez que vous souhaitez effectuer la sauvegarde à une date ultérieure plutôt qu'immédiate, vous pouvez cliquer sur **Schedule** (Planifier) à la place.

Étape 4 (Facultatif) Sélectionnez l'option **Encrypt File** (chiffrer le fichier) pour chiffrer le fichier de sauvegarde.

Si vous sélectionnez l'option, vous devez entrer le **mot de passe** qui sera nécessaire pour restaurer le fichier de sauvegarde (et **confirmer le mot de passe**).

Étape 5 (ISA 3000 uniquement.) Sélectionnez l'**emplacement des fichiers de sauvegarde**.

Vous pouvez créer la sauvegarde sur le **disque dur local** ou sur la **carte SD**. L'intérêt de l'utilisation de la carte SD est que vous pouvez l'utiliser pour récupérer la configuration sur un périphérique de remplacement.

Étape 6 Cliquez sur **Back Up Now** (Sauvegarder maintenant).

Le système démarre le processus de sauvegarde. Une fois la sauvegarde complétée, le fichier de sauvegarde s'affichera dans le tableau. Vous pouvez ensuite télécharger la copie de sauvegarde sur votre système et la stocker ailleurs, si vous le souhaitez.

Vous pouvez quitter la page de sauvegarde et de restauration après avoir lancé la sauvegarde. Cependant, le système sera probablement lent et vous devriez envisager de suspendre votre travail pour permettre à la sauvegarde de se terminer.

En outre, le système acquerra des verrous sur la base de données de configuration pendant une partie ou toute la sauvegarde, ce qui peut vous empêcher d'apporter des modifications pendant la durée du processus de sauvegarde.

Sauvegarder le système à une heure planifiée

Vous pouvez configurer une sauvegarde planifiée pour sauvegarder le système à une date et à une heure futures spécifiques. Une sauvegarde planifiée est une occurrence unique. Si vous souhaitez créer un calendrier de sauvegarde pour créer régulièrement des sauvegardes, configurez une sauvegarde récurrente au lieu d'une sauvegarde planifiée.



Remarque Si vous souhaitez supprimer la planification pour une sauvegarde future, modifiez la planification et cliquez sur **Remove** (Supprimer).

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (Afficher la configuration) dans le résumé Backup and Restore (Sauvegarde et restauration).

Étape 2 Cliquez sur **Scheduled Backup (Sauvegarde planifiée)** > **Schedule a Backup (Planifier une sauvegarde)**.

Si vous avez déjà une sauvegarde planifiée, cliquez sur **Scheduled Backup (Sauvegarde planifiée)** > **Edit (Modifier)**.

Étape 3 Entrez un nom pour la sauvegarde et, facultativement, une description.

Étape 4 Sélectionnez la date et l'heure de la sauvegarde.

Étape 5 (Facultatif) Sélectionnez l'option **Encrypt File** (chiffrer le fichier) pour chiffrer le fichier de sauvegarde.

Si vous sélectionnez l'option, vous devez entrer le **mot de passe** qui sera nécessaire pour restaurer le fichier de sauvegarde (et **confirmer le mot de passe**).

Étape 6 (ISA 3000 uniquement.) Sélectionnez l'**emplacement des fichiers de sauvegarde**.

Vous pouvez créer la sauvegarde sur le **disque dur local** ou sur la **carte SD**. L'intérêt de l'utilisation de la carte SD est que vous pouvez l'utiliser pour récupérer la configuration sur un périphérique de remplacement.

Étape 7 Cliquez sur **Schedule** (Planifier).

Lorsque la date et l'heure sélectionnées arrivent, le système effectue une sauvegarde. Une fois terminée, la copie de sauvegarde est répertoriée dans le tableau des sauvegardes.

Configuration d'une planification de sauvegarde récurrente

Vous pouvez configurer une sauvegarde récurrente pour sauvegarder le système à des intervalles réguliers. Par exemple, vous pourriez effectuer une sauvegarde tous les vendredis à minuit. Un calendrier de sauvegardes récurrentes vous permet de vous assurer que vous avez toujours un ensemble de sauvegardes récentes.



Remarque Si vous souhaitez supprimer une planification récurrente, modifiez la planification et cliquez sur **Remove** (Supprimer).

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuratio**n (Afficher la configuration) dans le résumé Backup and Restore (Sauvegarde et restauration).

Étape 2 Cliquez sur **Recurring Backup (Sauvegarde récurrente)** > **Configure (Configurer)**.

Si vous avez déjà configuré une sauvegarde récurrente, cliquez sur **Recurring Backup (Sauvegarde récurrente)** > **Edit (Modifier)**.

Étape 3 Entrez un nom pour la sauvegarde et, facultativement, une description.

Étape 4 Sélectionnez la **Frequency** (Fréquence) et le calendrier associé :

- **Daily**(Quotidien) : sélectionnez l'heure. Une sauvegarde est effectuée chaque jour à l'heure planifiée.
- **Weekly** (Hebdomadaire) : sélectionnez les jours de la semaine et l'heure. Une sauvegarde est effectuée chaque jour que vous sélectionnez à l'heure planifiée. Par exemple, vous pouvez planifier des sauvegardes chaque lundi, mercredi et vendredi à 23 h 00 (11 PM).
- **Monthly** (Mensuel) : sélectionnez les jours du mois et l'heure. Une sauvegarde est effectuée chaque jour que vous sélectionnez à l'heure planifiée. Par exemple, vous pouvez planifier des sauvegardes les 1er (1), 15e (15) et 28e (28) jours du mois à 23 h 00 (11 p.m.).

L'heure que vous précisez est ajustée selon l'heure avancée. Elle sera reculée ou avancée à chaque changement d'heure dans votre région. Vous devez modifier le calendrier au moment du changement d'heure si vous souhaitez conserver cette heure tout au long de l'année.

Étape 5 (Facultatif) Sélectionnez l'option **Encrypt File** (chiffrer le fichier) pour chiffrer le fichier de sauvegarde.

Si vous sélectionnez l'option, vous devez entrer le **mot de passe** qui sera nécessaire pour restaurer le fichier de sauvegarde (et **confirmer le mot de passe**).

Étape 6 (ISA 3000 uniquement.) Sélectionnez l'**emplacement des fichiers de sauvegarde**.

Vous pouvez créer la sauvegarde sur le **disque dur local** ou sur la **carte SD**. L'intérêt de l'utilisation de la carte SD est que vous pouvez l'utiliser pour récupérer la configuration sur un périphérique de remplacement.

Étape 7 Cliquez sur **Save** (enregistrer).

Lorsque les dates et heures sélectionnées arrivent, le système effectue une sauvegarde. Une fois terminée, la copie de sauvegarde est répertoriée dans le tableau des sauvegardes.

La planification récurrente continue d'effectuer des sauvegardes jusqu'à ce que vous la changiez ou la supprimiez.

Restauration d'une sauvegarde

Vous pouvez restaurer les sauvegardes au besoin tant que le périphérique exécute la même version du logiciel (y compris le numéro de build) que celle qu'il exécutait au moment où vous avez effectué la sauvegarde. Vous pouvez restaurer une sauvegarde sur un périphérique de remplacement uniquement si les deux périphériques sont du même modèle et exécutent la même version du logiciel (y compris le numéro de build).

Cependant, vous ne pouvez pas restaurer une sauvegarde si le périphérique fait partie d'un pair à haute disponibilité. Vous devez d'abord interrompre la haute disponibilité à partir de la page **Device (périphérique)** > **High Availability (haute disponibilité)**, puis vous pourrez restaurer la sauvegarde. Si la sauvegarde comprend la configuration à haute disponibilité, le périphérique rejoindra le groupe à haute disponibilité. Ne restaurez pas la même sauvegarde sur les deux unités, car elles deviendraient alors actives. Au lieu de cela, restaurez la sauvegarde sur l'unité que vous souhaitez rendre active en premier, puis restaurez la sauvegarde équivalente sur l'autre unité.

Si la copie de sauvegarde que vous souhaitez restaurer ne se trouve pas déjà sur le périphérique, vous devez d'abord téléverser la sauvegarde avant de la restaurer.

Pendant une restauration, le système est complètement indisponible.

Remarque La sauvegarde n'inclut pas la configuration de l'adresse IP de gestion. Ainsi, lorsque vous récupérez un fichier de sauvegarde, l'adresse de gestion n'est pas remplacée à partir de la copie de sauvegarde. Cela garantit que toutes les modifications que vous avez apportées à l'adresse sont conservées et permet également de restaurer la configuration sur un périphérique différent sur un segment de réseau différent. La sauvegarde ne comprend pas non plus les informations de licence ou d'enregistrement dans le nuage, de sorte que tout état de licence ou d'enregistrement dans le nuage qui existe au moment de la restauration est conservé.

Avant de commencer

Si vous restaurez une sauvegarde sur un système différent, par exemple lors du remplacement d'un périphérique, la meilleure pratique consiste d'abord à enregistrer le périphérique et à activer les licences facultatives requises par les fonctionnalités configurées dans le fichier de sauvegarde. Le fichier de sauvegarde ne comprend pas les renseignements sur les licences ni sur les services dans le nuage. Ainsi, les modifications de licences ou les enregistrements dans le nuage que vous effectuez avant la restauration sont conservés.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuratio**n (Afficher la configuration) dans le résumé Backup and Restore (Sauvegarde et restauration).

Cela ouvre la page Backup and Restore (Sauvegarde et restauration). Le tableau répertorie toutes les copies de sauvegarde existantes qui sont disponibles sur le système.

Étape 2 Si la copie de sauvegarde que vous souhaitez restaurer ne figure pas dans la liste des sauvegardes disponibles, cliquez sur **Upload (Charger)** > **Browse (Parcourir)** et chargez la copie de sauvegarde.

Étape 3 Cliquez sur l'icône de restauration ( ) pour le fichier.

Vous êtes invité à confirmer la restauration. Par défaut, la copie de sauvegarde sera supprimée après la restauration, mais vous pouvez sélectionner **Do not remove the backup after restoring** (Ne pas supprimer la sauvegarde après la restauration) pour la conserver avant de poursuivre la restauration.

Si le fichier de sauvegarde a été chiffré, vous devez saisir le **Password (mot de passe)** requis pour ouvrir le fichier et le déchiffrer.

Le système redémarrera une fois la restauration terminée.

Remarque
Après le redémarrage, le système vérifie automatiquement les mises à jour de Vulnerability Database (base de données relative aux vulnérabilités) (VDB), de Geolocation (Géolocalisation) et de la base de données Rules (Règles), et les télécharge au besoin. Comme ces mises à jour peuvent être volumineuses, la tentative initiale peut échouer. Veuillez vérifier la liste des tâches et, si un téléchargement échoue, téléchargez manuellement une mise à jour, comme décrit dans Mise à jour des bases de données du système., à la page 821 Le système redéploie également les politiques. Tout déploiement ultérieur échouera tant que la mise à jour n'aura pas été effectuée avec succès.

Étape 4 Si nécessaire, cliquez sur **Device (Périphérique)** > **Smart License (Licence Smart)** > **View Configuration (Afficher la configuration)**, réenregistrez le périphérique et réactivez les licences facultatives requises.

La sauvegarde n'inclut pas les informations de licence ni d'enregistrement dans le nuage. Ainsi, si vous restaurez une sauvegarde sur un nouveau système, par exemple lors du remplacement d'un périphérique, et que le système est en mode d'évaluation, vous devez l'enregistrer et activer les licences dont vous avez besoin. Si vous avez enregistré le périphérique et activé les licences avant la restauration, aucune modification supplémentaire n'est requise.

Si vous restaurez simplement une sauvegarde précédente sur le même système, vous ne devriez pas avoir à apporter de modifications aux licences ou à l'enregistrement dans le nuage. Cependant, vérifiez que toutes les licences facultatives nécessaires sont activées, car la sauvegarde pourrait inclure des fonctionnalités nécessitant des licences que vous avez désactivées après la création de la sauvegarde.

Gestion des fichiers de sauvegarde

Lorsque vous créez de nouvelles sauvegardes, les fichiers de sauvegarde sont répertoriés sur la page Backup and Restore (Sauvegarde et restauration). Les copies de sauvegarde ne sont pas conservées indéfiniment : lorsque l'utilisation de l'espace disque sur le périphérique atteint le seuil maximal, les anciennes copies de sauvegarde sont supprimées pour faire place aux plus récentes. En outre, lorsque vous installez une mise à niveau autre qu'un correctif rapide, tous les fichiers de sauvegarde sont supprimés. Ainsi, vous devez gérer régulièrement les fichiers de sauvegarde pour vous assurer d'avoir les copies de sauvegarde spécifiques que vous souhaitez conserver.

Vous pouvez effectuer les opérations suivantes pour gérer vos copies de sauvegarde :

- Télécharger des fichiers vers un stockage sécurisé : pour télécharger un fichier de sauvegarde sur votre poste de travail, cliquez sur l'icône de téléchargement ( ) en regard du fichier. Vous pouvez ensuite déplacer le fichier vers votre stockage sécurisé.

- Charger un fichier de sauvegarde dans le système : si vous souhaitez restaurer une copie de sauvegarde qui n'est plus disponible sur le périphérique, cliquez sur **Upload (Charger)** > **Browse File (Parcourir le fichier)**, puis chargez-le depuis votre poste de travail. Vous pouvez ensuite le restaurer.

Remarque Les fichiers chargés peuvent être renommés pour correspondre au nom de fichier d'origine. De plus, s'il y a déjà plus de 3 copies de sauvegarde sur le système, la plus ancienne sera supprimée pour faire de l'espace pour le fichier téléchargé. Vous ne pouvez pas téléverser de fichiers qui ont été créés par une ancienne version de logiciel.

- Restaurer une sauvegarde : pour restaurer une copie de sauvegarde, cliquez sur l'icône de restauration ( ) pour le fichier. Le système n'est pas disponible pendant la restauration et redémarrera une fois la restauration terminée. Vous devez déployer la configuration une fois que le système est opérationnel.
- Supprimer un fichier de sauvegarde : si vous ne souhaitez plus effectuer de sauvegarde en particulier, cliquez sur l'icône de suppression ( ) pour le fichier. Vous êtes invité à confirmer la suppression. Une fois supprimé, vous ne pouvez pas récupérer le fichier de sauvegarde.

Audit et gestion du changement

Vous pouvez afficher les informations d'état sur les événements du système et les actions que les utilisateurs ont effectuées. Ces informations peuvent vous aider à effectuer l'audit du système et à vous assurer qu'il est géré correctement.

Cliquez sur **Device (Périphérique)** > **Device Administration (Administration du périphérique)** > **Audit Log (Journal d'audit)** pour voir le journal d'audit. En outre, vous pouvez trouver des renseignements sur la gestion du système en cliquant sur les boutons de l'icône **Task List** (Liste des tâches) ou **Deployment** (Déploiement) dans le coin supérieur droit.

Les rubriques suivantes couvrent certains des concepts et tâches principaux d'audit du système et de gestion des changements.

Événements d'audit

Le journal d'audit peut inclure les types d'événements suivants :

Événement de mise à jour du flux personnalisé, échec de la mise à jour du flux personnalisé

Ces événements indiquent une mise à jour réussie ou un échec d'un flux de Security Intelligence personnalisé. Les détails comprennent qui a lancé la mise à jour et des renseignements sur le flux qui a été mis à jour.

Événement du résumé de l'importation du fichier de règles personnalisées

Ces événements indiquent que vous avez importé un fichier qui contient une ou plusieurs règles de prévention des intrusions personnalisées. L'événement comprend un résumé du nombre de règles ajoutées, mises à jour et supprimées, ainsi qu'une vue sur les différences qui affiche les détails des règles importées.

Deployment Completed (Déploiement terminé), Deployment Failed (Échec du déploiement) : ***job name*** **(nom de la tâche) ou** ***entity name*** **(nom d'entité)**

Ces événements indiquent une tâche de déploiement terminée ou échouée. Les détails comprennent qui a lancé la tâche et des informations sur l'entité de tâche. Les tâches ayant échoué comprennent le message d'erreur lié à la défaillance.

Les détails comprennent également un onglet **Differences View (Affichage des différences)**, qui affiche les modifications qui ont été déployées sur le périphérique dans la tâche. Il s'agit de la combinaison de tous les événements de modification d'entité pour les entités déployées.

Pour filtrer en fonction de ces événements, cliquez simplement sur le filtre prédéfini **Deployment History** (Historique de déploiement). Notez que le type d'événement pour ces événements est un événement de déploiement, vous ne pouvez pas filtrer en fonction des événements terminés ou échoués uniquement.

Le nom de l'événement comprend le nom de la tâche défini par l'utilisateur (si vous en configurez un), ou « Utilisateur (*nom d'utilisateur*) déployé pour le déploiement ». Il existe également des tâches « Device Setup Automatic Deployment (Déploiement automatique de la configuration du périphérique) » et « Device Setup Automatic Deployment (Final Step) (Déploiement automatique de la configuration du périphérique – dernière étape) » qui se produisent pendant l'assistant de configuration du périphérique.

Entity Created (Entité créée), Entity Updated (Entité mise à jour), Entity Deleted (Entité supprimée) : ***nom d'entité*** **(***type d'entité***)**

Ces événements indiquent qu'une modification a été apportée à l'entité ou à l'objet identifié. Les détails de l'entité comprennent qui a effectué la modification, ainsi que le nom, le type et l'ID de l'entité. Vous pouvez filtrer en fonction de ces éléments. Les détails comprennent également un onglet **Differences View** (Affichage des différences), qui affiche les modifications apportées à l'objet.

Événement d'action à haute disponibilité

Ces événements sont liés à des actions sur la configuration à haute disponibilité, soit des actions que vous avez lancées, soit des actions que le système a lancées. HA Action Event (Événement d'action HA) est le type d'événement, mais les noms d'événements sont l'un des suivants :

- **HA Suspended** (HA suspendue) : vous avez suspendu intentionnellement la haute disponibilité sur le système.
- **HA Resumed** (HA reprise) : vous avez repris intentionnellement la haute disponibilité sur le système.
- **HA Reset** (HA réinitialisée) : vous avez réinitialisé intentionnellement la haute disponibilité sur le système.
- **HA Failover: Unit Switched Modes** (Basculement HA : unité ayant changé de mode) : vous avez changé de mode intentionnellement ou le système a basculé en raison de violations des mesures d'intégrité. Le message indique que l'homologue actif est devenu en veille ou que l'homologue en veille est devenu actif.

High Availability Sync Completed (Synchronisation de la haute disponibilité terminée)

L'unité active a synchronisé la configuration avec l'unité en veille. L'événement comprend les informations de modification pour la version précédente par rapport à la version synchronisée.

Liste des interfaces analysée

Cet événement indique que vous avez recherché des modifications dans l'inventaire des interfaces.

Modifications en attente annulées

Cet événement indique que vous avez supprimé toutes les modifications en attente. Toutes les modifications indiquées dans les événements Entity Created (Entité créée), Entity Updated (Entité mise à jour) et Entity Deleted (Entité supprimée), entre cet événement et l'événement Deployment Completed (Déploiement terminé), sont supprimées, et l'état des objets concernés est rétabli à la dernière version déployée.

Événement de mise à jour des règles

Lors de l'exécution de Snort 3, cet événement de l'entité LSPUpdateServer affiche des informations détaillées sur les règles de prévention des intrusions qui ont été ajoutées, supprimées ou modifiées lors du téléchargement et de l'installation d'un nouvel ensemble de règles de prévention des intrusions. L'événement est limité à 100 règles, donc si plus de 100 sont ajoutées, supprimées ou modifiées, l'événement ne contiendra pas d'informations complètes. Cet événement ne s'affiche pas pour les mises à jour de Snort 2.

Task Started (Tâche démarrée), Task Completed (Tâche terminée), Task Failed (Tâche échouée)

Les événements de tâche indiquent le début et la fin d'une tâche lancée par le système ou un utilisateur. Ces deux événements sont regroupés en une seule tâche dans la liste des tâches, que vous pouvez voir en cliquant sur le bouton **Task List** (Liste des tâches) dans le coin supérieur droit.



Les tâches comprennent des actions telles que les tâches de déploiement et les mises à jour manuelles ou planifiées de la base de données. Tout élément dans la liste des tâches correspondra à deux événements de tâche dans le journal d'audit, une indication du début de la tâche et un achèvement réussi ou un échec.

User Logged In (Utilisateur connecté), User Logged Out (Utilisateur déconnecté) : ***nom d'utilisateur***

Ces événements affichent l'heure et l'adresse IP source de l'utilisateur qui se connecte et se déconnecte de Gestionnaire de périphériques de pare-feu. L'événement Déconnexion de l'utilisateur se produit à la fois pour les déconnexions actives et les déconnexions automatiques en raison du dépassement du temps d'inactivité.

Ces événements ne sont pas liés aux utilisateurs de VPN d'accès à distance qui établissent des connexions avec le périphérique. Ils n'incluent pas non plus la connexion et la déconnexion à l'interface de ligne de commande du périphérique.

Visualisation et analyse du journal d'audit

Le journal d'audit comprend des informations sur les événements lancés par le système et par l'utilisateur, tels que les tâches de déploiement, les mises à jour de la base de données et les connexions/déconnexions de Gestionnaire de périphériques de pare-feu.

Pour obtenir une explication des types d'événement que vous pouvez voir dans le journal, consultez Événements d'audit, à la page 836.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis sur le lien **Device Administration (Administration du périphérique)** > **View Configuration (Afficher la configuration)**.

Étape 2 Cliquez sur **Audit Log** (Journal d'audit) dans la table des matières s'il n'est pas déjà sélectionné.

Les événements sont regroupés par date et, dans une journée, par heure, la date et l'heure les plus récentes en haut de la liste. Au départ, chaque événement est réduit, de sorte que vous ne voyez que l'heure, le nom de l'événement, l'utilisateur qui a lancé l'événement et l'adresse IP source de l'utilisateur. « Système » pour l'utilisateur et l'adresse IP signifie que le périphérique lui-même a lancé l'événement.

Vous pouvez effectuer les opérations suivantes :

- Cliquez sur > à côté du nom de l'événement pour l'ouvrir et voir les détails de l'événement. Cliquez à nouveau sur l'icône pour fermer l'événement. De nombreux événements ont une liste simple d'attributs d'événement, tels que le type d'événement, le nom d'utilisateur, l'adresse IP source, etc. Cependant, les événements d'entité et de déploiement ont deux onglets :
  - **Summary** (Résumé) affiche les attributs de base de l'événement.
  - **Differences View** (Affichage des différences) affiche une comparaison de la configuration « déployée » existante avec les modifications apportées dans le cadre de l'événement. Pour les tâches de déploiement, cet affichage peut être long et nécessiter un défilement. Il résume toutes les différences par rapport aux modifications d'événements d'entité qui ont fait partie de la tâche de déploiement.
- Sélectionnez une plage temporelle différente dans la liste déroulante à droite du champ de filtre. La valeur par défaut est d'afficher les événements des 2 dernières semaines, mais vous pouvez modifier cela pour les dernières 24 heures, 7 jours, mois ou 6 mois. Cliquez sur **Custom** (Personnalisé) pour spécifier une plage exacte en saisissant la date et l'heure de début et de fin.
- Cliquez sur n'importe quel lien dans le journal pour ajouter un filtre de recherche pour cet élément. La liste est mise à jour de sorte que seuls les événements qui comprennent l'élément sont affichés. Vous pouvez également simplement cliquer dans la zone **Filter** (Filtre) et créer un filtre directement. Il existe des filtres prédéfinis sous la zone de filtre, sur lesquels vous pouvez cliquer pour charger les critères de filtrage correspondants. Pour des informations détaillées sur le filtrage des événements, consultez Filtrage du journal d'audit, à la page 839.
- Rechargez la page du navigateur pour actualiser le journal avec les derniers événements.

Filtrage du journal d'audit

Vous pouvez appliquer un filtre au journal d'audit pour restreindre votre affichage à certains types de messages uniquement. Chaque élément du filtre doit correspondre exactement et entièrement. Par exemple, « User = admin » (Utilisateur = admin) n'affiche que les événements déclenchés par l'utilisateur nommé **admin**.

Vous pouvez utiliser les techniques suivantes, seules ou en combinaison, pour créer un filtre. La liste est automatiquement mise à jour chaque fois que vous ajoutez un élément de filtre.

Cliquez sur Predefined Filter (Filtre prédéfini).

Sous le champ **Filter** (Filtre) se trouvent les filtres prédéfinis. Cliquez simplement sur un lien pour charger le filtre. Vous êtes invité à confirmer. Si un filtre est déjà appliqué, il est remplacé ; il n'est pas complété.

Cliquer sur les éléments en surbrillance

La façon la plus simple de créer un filtre est de cliquer sur les éléments dans le tableau de journaux ou les détails des événements qui contiennent les valeurs sur lesquelles vous avez l'intention de filtrer.

Cliquez sur un élément pour mettre à jour le champ **Filter** (Filtre) avec un élément correctement formaté pour cette combinaison de valeur et d'élément. Cependant, l'utilisation de cette technique nécessite que la liste d'événements existante contienne les valeurs souhaitées.

Si vous pouvez ajouter un élément de filtre pour un élément, l'élément est souligné lorsque vous passez le curseur dessus et vous voyez la commande **Click to Add to Filter** (Cliquer pour ajouter au filtre).

Sélection d'éléments atomiques

Vous pouvez également créer un filtre en cliquant dans le champ **Filter** (Filtre) et en sélectionnant l'élément atomique souhaité dans la liste déroulante, en saisissant la valeur de correspondance après le signe égal, puis en appuyant sur Enter (Entrée). Vous pouvez filtrer en fonction des éléments suivants. Notez que tous les éléments ne sont pas pertinents pour chaque type d'événement.

- **Event Type** (Type d'événement) : il s'agit généralement, mais pas toujours, du même élément que le nom de l'événement (sans qualificatifs variables comme le nom d'entité ou l'utilisateur). Pour les événements de déploiement, le type d'événement est Deployment Event (Événement de déploiement). Pour obtenir une explication des types d'événements, consultez Événements d'audit, à la page 836.
- **User** (Utilisateur) : le nom de l'utilisateur qui a initié l'événement. L'utilisateur du système est écrit en majuscules : SYSTEM.
- **Source IP (IP source)** : l'adresse IP à partir de laquelle l'utilisateur a initié l'événement. L'adresse IP source des événements initiés par le système est SYSTEM.
- **Entity ID** (ID d'entité) : l'UUID de l'entité ou de l'objet, qui est une longue chaîne illisible, telle que 8e7021b4-2e1e-11e8-9e5d-0fc002c5f931. Normalement, pour utiliser ce filtre, vous devez soit cliquer sur un ID d'entité dans les détails d'un événement, soit récupérer l'ID nécessaire par le biais d'un appel GET pertinent utilisant l'API REST.
- **Entity Name** (Nom d'entité) : le nom de l'entité ou de l'objet. Pour les entités créées par l'utilisateur, il s'agit généralement du nom que vous avez donné à l'objet, par exemple, InsideNetwork pour un objet réseau. Pour les entités générées par le système ou, dans certains cas, les entités définies par l'utilisateur, il s'agit d'un nom prédéfini mais intelligible, par exemple, « Déploiement déclenché par l'utilisateur (admin) » pour les tâches de déploiement que vous ne nommez pas explicitement.
- **Entity Type** (Type d'entité) : le type d'entité ou d'objet. Il s'agit de noms prédéfinis, mais intelligibles, comme Network Object (Objet réseau). Vous pouvez trouver des types d'entités dans l'explorateur d'API en examinant le modèle d'objet pertinent pour la valeur de « type ». Les types d'API sont normalement tous en minuscules sans espaces. Si vous les saisissez exactement comme indiqué dans le modèle, la chaîne passe à un format plus lisible lorsque vous appuyez sur Entrée. La saisie dans l'un ou l'autre des formats fonctionne. Pour ouvrir l'explorateur d'API, cliquez sur le bouton more options (plus d'options) (⋮) et choisissez **API Explorer** (Explorateur d'API).

Règles pour les filtres de journal d'audit complexes

Lors de la création d'un filtre complexe qui contient plus d'un élément atomique, gardez les règles suivantes à l'esprit :

- Les éléments du même type ont une relation OU entre toutes les valeurs de ce type. Par exemple, l'inclusion de « User = admin » et « User = SYSTEM » correspond aux événements qui ont été lancés par l'un ou l'autre des utilisateurs.

- Les éléments de différents types ont une relation ET. Par exemple, inclure « Type d'événement = Entité mise à jour » et « Utilisateur = SYSTEM » affiche uniquement les événements pour lesquels le système a mis à jour une entité plutôt qu'un utilisateur actif.
- Vous ne pouvez pas utiliser de caractères génériques, d'expressions régulières, de correspondances partielles ou de correspondances de chaîne de texte simples.

Examen du déploiement et de l'historique des modifications d'entité

Les événements de déploiement et d'entité comprennent un onglet **Differences View** (Affichage des différences) dans les détails de l'événement. Cet onglet affiche une comparaison codée par couleur de l'ancienne configuration avec les modifications.

- Pour les tâches de déploiement, il s'agit d'une comparaison de la configuration exécutée sur le périphérique avant le déploiement avec les modifications effectivement déployées.
- Pour les événements d'entité, il s'agit des modifications de configuration apportées à la version précédente de l'objet. La version précédente peut être la version actuellement présente sur le périphérique, ou il peut s'agir d'un changement apporté à un objet qui n'a pas encore été déployé.

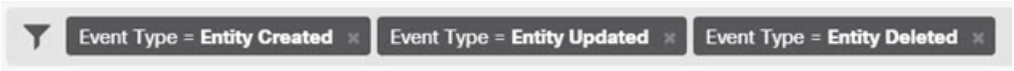
Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis sur le lien **Device Administration (Administration du périphérique)** > **View Configuration (Afficher la configuration)**.

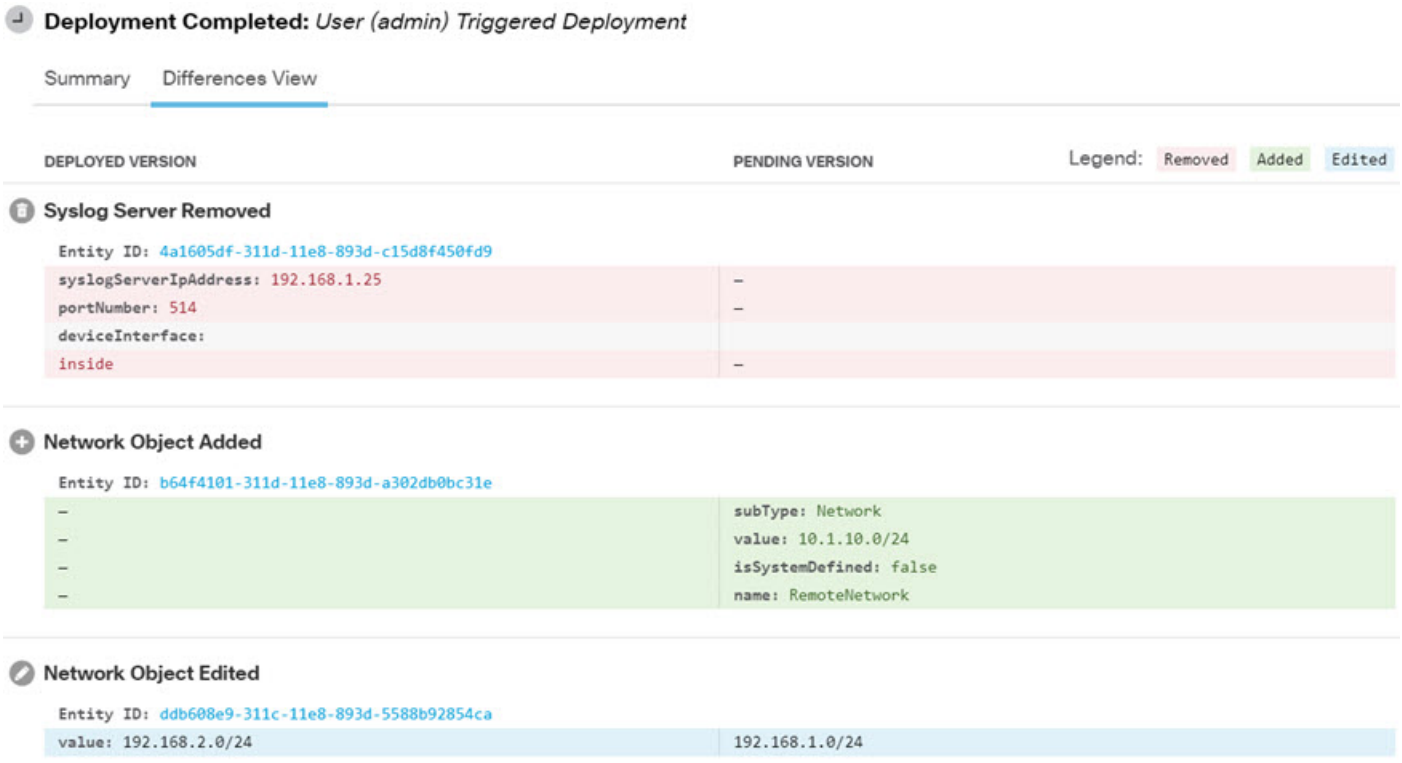
Étape 2 Cliquez sur **Audit Log** (Journal d'audit) dans la table des matières s'il n'est pas déjà sélectionné.

Étape 3 (Facultatif) Filtrer les messages :

- Événements de déploiement : cliquez sur le filtre prédéfini **Deployment History** (Historique de déploiement) dans la zone de filtre.
- Événements de modification d'entité : créez manuellement un filtre à l'aide de l'élément Event Type (Type d'événement) pour le type de modification qui vous intéresse. Pour voir toutes les modifications d'entités, incluez trois spécifications pour l'entité créée, l'entité mise à jour et l'entité supprimée. Le filtre ressemblerait à ce qui suit :



Étape 4 Ouvrez l'événement et cliquez sur l'onglet **Differences View** (Affichage des différences).



Les modifications sont codées par couleur et l'en-tête indique le type d'objet et s'il a été ajouté (Created (Créé)), supprimé (Deleted (Supprimé)) ou modifié (Updated (Mis à jour)). Les objets modifiés affichent uniquement les attributs qui ont été modifiés ou supprimés de l'objet. Dans les tâches de déploiement, il existe des en-têtes distincts pour chaque entité modifiée. L'en-tête indique le type d'entité de l'objet.

Annuler toutes les modifications en attente

Si vous n'êtes pas satisfait d'un ensemble de modifications de configuration qui n'ont pas encore été déployées, vous pouvez annuler toutes les modifications en attente. Ainsi, toutes les fonctionnalités sont restaurées à l'état qui existe sur le périphérique. Vous pouvez ensuite recommencer avec vos modifications de configuration.

Procédure

Étape 1 Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

L'icône est mise en évidence avec un point lorsqu'il y a des modifications en attente.



Étape 2 Cliquez sur **More Options (Plus d'options)** > **Discard All (Ignorer tout)**.

Étape 3 Cliquez sur **OK** dans la boîte de dialogue de confirmation.

Le système annule les modifications, et vous verrez un message indiquant qu'il n'y a aucune modification en attente une fois le processus terminé. Le système ajoute un événement Modifications en attente ignorées au journal d'audit.

Exporter la configuration du périphérique.

Téléchargez une copie de la configuration actuellement déployée au format JSON. Vous pouvez utiliser le fichier à des fins d'archivage ou de conservation des données. Toutes les données sensibles, telles que les mots de passe et les clés secrètes, sont masquées.

Vous ne pouvez pas importer le fichier dans cet appareil ou dans un autre appareil. Cette fonction ne remplace pas la sauvegarde du système.

Vous devez avoir effectué au moins une tâche de déploiement réussie avant de pouvoir télécharger la configuration.

Procédure

Étape 1 Choisissez **Device** (Périphérique), puis cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device Administration** (Administration du périphérique).

Étape 2 Cliquez sur **Download Configuration** (Télécharger la configuration) dans la table des matières.

Étape 3 Cliquez sur **Get Device Configuration** (Obtenir la configuration du périphérique) pour lancer une tâche qui crée le fichier.

Si vous avez déjà créé un fichier, vous verrez un bouton de téléchargement et le message **File is ready to download** (Le fichier est prêt à être téléchargé), avec la date de création du fichier.

Selon la taille de la configuration, la génération du fichier peut prendre plusieurs minutes. Vérifiez la liste des tâches ou le journal d'audit, ou revenez à cette page périodiquement, jusqu'à ce que la tâche d'exportation de la configuration soit terminée et que le fichier soit généré.

Étape 4 Lorsque le fichier est généré, revenez à cette page et cliquez sur le bouton **Download the Configuration File** (Télécharger le fichier de configuration) ( ) pour enregistrer le fichier sur votre poste de travail.

Gestion du Gestionnaire de périphériques de pare-feu et accès des utilisateurs Firewall Threat Defense

Vous pouvez configurer une source d'authentification et d'autorisation externe pour que les utilisateurs puissent se connecter à Firewall Threat Defense (accès HTTPS). Vous pouvez utiliser un serveur externe en plus ou à la place de la base de données des utilisateurs locaux et de l'utilisateur **admin** défini par le système. Notez que vous ne pouvez pas créer de comptes utilisateurs locaux supplémentaires pour l'accès Gestionnaire de périphériques de pare-feu.

Bien que vous puissiez avoir plusieurs comptes d'utilisateurs Gestionnaire de périphériques de pare-feu externes qui peuvent modifier la configuration, ces modifications ne sont pas suivies par utilisateur. Lorsqu'un utilisateur déploie des changements, les modifications effectuées par tous les utilisateurs sont déployées. Il n'y a aucun verrouillage : c'est-à-dire que plus d'un utilisateur peut tenter de mettre à jour le même objet en même temps, ce qui entraînera l'enregistrement d'un changement par un seul utilisateur. Vous ne pouvez pas non plus ignorer les modifications en fonction de l'utilisateur.

Vous pouvez avoir cinq sessions utilisateur simultanées. Si un sixième utilisateur se connecte, la session utilisateur la plus ancienne est automatiquement déconnectée. Il y a également un délai d'inactivité qui déconnecte les utilisateurs inactifs après 20 minutes.

Vous pouvez également configurer l'authentification et l'autorisation externes pour l'accès SSH à l'interface de ligne de commande Firepower Threat Defense. La base de données locale est toujours vérifiée avant d'utiliser la source externe. Vous pouvez donc créer des utilisateurs locaux supplémentaires pour un accès sécurisé. Ne créez pas d'utilisateurs en double dans la source locale et externe. À l'exception de l'utilisateur admin **admin**, il n'y a pas de croisement entre l'interface de ligne de commande et les utilisateurs Gestionnaire de périphériques de pare-feu : les comptes d'utilisateurs sont complètement séparés.



Remarque Lorsque vous utilisez des serveurs externes, vous pouvez contrôler l'accès par utilisateur au niveau des sous-ensembles de vos périphériques en configurant des groupes de serveurs AAA distincts ou en créant des politiques d'authentification et d'autorisation dans les serveurs AAA qui permettent à l'utilisateur d'accéder uniquement à certaines adresses IP du périphériqueFirepower Threat Defense.

Les rubriques suivantes expliquent comment configurer et gérer l'accès utilisateur Gestionnaire de périphériques de pare-feu et l'accès utilisateur de l'interface de ligne de commande.

Configuration de l'autorisation externe (AAA) pour les utilisateurs HTTPS Gestionnaire de périphériques de pare-feu

Vous pouvez fournir un accès HTTPS à Gestionnaire de périphériques de pare-feu à partir d'un serveur AAA externe. En activant l'authentification et l'autorisation AAA, vous pouvez fournir différents niveaux de droits d'accès et ne pas demander à chaque utilisateur de se connecter avec le compte **admin** local.

Ces utilisateurs externes sont également autorisés pour l'API Firewall Threat Defense et l'API Explorer.

Vous pouvez fournir un contrôle d'accès basé sur les rôles (RBAC) en configurant l'autorisation pour les utilisateurs de gestion dans le serveur AAA. Les niveaux varient selon le type de serveur. Lorsqu'un utilisateur se connecte à Gestionnaire de périphériques de pare-feu, le nom d'utilisateur et le rôle sont affichés dans le coin supérieur droit de la page. Après avoir configuré les comptes correctement sur le serveur AAA, vous pouvez l'activer pour un accès administratif en utilisant cette procédure.

Autorisation utilisateur RADIUS

Pour fournir un contrôle d'accès basé sur les rôles, mettez à jour les comptes d'utilisateurs sur votre serveur RADIUS pour définir l'attribut **cisco-av-pair** (dans ISE, mais l'attribut est écrit Cisco-AVPair dans RADIUS gratuit; vérifiez votre système pour vérifier si l'écriture est correcte). Cet attribut doit être défini correctement sur un compte utilisateur, sinon l'utilisateur se voit refuser l'accès à l'API REST.Gestionnaire de périphériques de pare-feu Voici les valeurs suivantes prises en charge pour l'attribut **cisco-av-pair** :

- **fdm.userrole.authority.admin** fournit un accès administrateur complet. Ces utilisateurs peuvent effectuer toutes les actions que l'utilisateur **admin** local peut effectuer.

- **fdm.userrole.authority.rw** fournit un accès en lecture-écriture. Ces utilisateurs peuvent faire tout ce qu'un utilisateur en lecture seule peut faire, ainsi que modifier et déployer la configuration. Les seules restrictions concernent les actions critiques pour le système, qui comprennent l'installation des mises à niveau, la création et la restauration de sauvegardes, et la déconnexion des utilisateurs de Gestionnaire de périphériques de pare-feu.
- **fdm.userrole.authority.ro** fournit un accès en lecture seule. Ces utilisateurs peuvent afficher les tableaux de bord et la configuration, mais ne peuvent apporter aucune modification. Si l'utilisateur tente d'apporter une modification, le message d'erreur explique que cela est causé par un manque d'autorisation.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis cliquez sur le lien**System Settings** > **Management Access**.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **Management Access List** (liste d'accès de gestion) dans la table des matières.

Étape 2 Cliquez sur l'onglet **AAA Configuration** s'il n'est pas déjà sélectionné.

Étape 3 Configurez les options (**HTTPS Connection (Connexion HTTPS)**) :

- **Server Group for Management/REST API** (Groupe de serveurs pour la gestion/l'API REST) : sélectionnez le groupe de serveurs (pour l'authentification/autorisation externe) ou la base de données d'utilisateurs locaux LocalIdentitySource (LocalIdentitySource) que vous souhaitez utiliser comme source d'authentification principale.

  Si le groupe de serveurs n'existe pas encore, cliquez sur le lien pour créer un nouveau groupe et créez-le maintenant. Pour RADIUS, vous devrez également créer des objets de serveur pour chaque serveur, afin de les ajouter au groupe, mais vous pouvez le faire tout en définissant le groupe de serveurs. Pour en savoir plus sur RADIUS, consultez Serveurs et groupes RADIUS, à la page 176.

- **Authentication with LOCAL (Authentification avec LOCAL)** (RADIUS.)—Si vous sélectionnez un groupe de serveurs RADIUS externes, vous pouvez spécifier comment utiliser la source d'identité locale, qui contient le compte utilisateur local **admin**. Sélectionnez l'une des options suivantes :
  - **Before External Server** (Avant le serveur externe) : le système vérifie d'abord le nom d'utilisateur et le mot de passe par rapport à la source locale.
  - **After External Server** (Après le serveur externe) : la source locale est vérifiée uniquement si la source externe n'est pas disponible.
  - **Never** (Jamais) : (non recommandé.) La source locale n'est jamais utilisée, vous ne pouvez donc pas vous connecter en tant qu'utilisateur admin.

    Mise en garde
    Si vous sélectionnez **Never** (Jamais), vous ne pourrez pas vous connecter au Gestionnaire de périphériques de pare-feu en utilisant le compte **admin**. Vous serez verrouillé hors du système si le serveur AAA devient indisponible ou si vous configurez mal les comptes dans le serveur AAA.

Étape 4 Cliquez sur **Save** (Enregistrer).

Configuration de l'autorisation externe (AAA) pour les utilisateurs de l'interface de commande (SSH) Firewall Threat Defense

Vous pouvez fournir un accès SSH à l'interface de ligne de commande Firewall Threat Defense à partir d'un serveur RADIUS externe. En activant l'authentification et l'autorisation RADIUS, vous pouvez fournir différents niveaux de droits d'accès à partir d'une source d'authentification unique, plutôt que de définir des comptes d'utilisateurs locaux distincts sur chaque appareil.

Ces utilisateurs externes SSH ne sont **pas** autorisés pour l'API Firewall Threat Defense et l'API Explorer. Le mécanisme que vous utilisez pour définir l'autorisation SSH est différent de celui requis pour l'accès HTTPS. Cependant, vous pouvez configurer le même utilisateur RADIUS avec les critères d'authentification SSH et HTTPS, de sorte qu'un utilisateur donné puisse accéder au système via les deux protocoles.

Pour fournir un contrôle d'accès basé sur les rôles (RBAC) pour l'accès SSH, mettez à jour les comptes d'utilisateur sur votre serveur RADIUS pour définir l'attribut de type de service (**Service-Type**). Cet attribut doit être défini sur un compte utilisateur, sinon l'utilisateur se voit refuser l'accès SSH au périphérique. Voici les valeurs suivantes prises en charge pour l'attribut **Service-Type** :

- **Administratif (6)** : Fournit une autorisation d'accès de **configuration** au niveau de l'interface de ligne de commande. Ces utilisateurs peuvent utiliser toutes les commandes de l'interface de ligne de commande.
- **NAS Prompt (7)** ou tout autre niveau que 6 : Fournit une autorisation d'accès de **base** au niveau de l'interface de ligne de commande. Ces utilisateurs peuvent utiliser des commandes de lecture seule, comme les commandes **show**, à des fins de surveillance et de dépannage.

Après avoir configuré les comptes correctement sur le serveur RADIUS, vous pouvez l'activer pour un accès administratif SSH à l'aide de cette procédure.



Remarque Ne créez pas d'utilisateurs en double dans la source locale et externe. Si vous créez des noms d'utilisateur en double, assurez-vous qu'ils ont les mêmes droits d'autorisation. Vous ne pouvez pas vous connecter en utilisant le mot de passe de la version externe du compte d'utilisateur lorsque les droits d'autorisation diffèrent dans le compte d'utilisateur local; vous pouvez vous connecter en utilisant uniquement le mot de passe local. Si les droits sont identiques, le mot de passe que vous utilisez détermine si vous êtes connecté en tant qu'utilisateur externe ou local, en supposant que les mots de passe sont différents. Même si la base de données locale est vérifiée en premier, si un nom d'utilisateur existe dans la base de données locale mais que le mot de passe est incorrect, le serveur externe est vérifié, et si le mot de passe est correct pour la source externe, la connexion réussira.

Avant de commencer

Veuillez informer les utilisateurs définis en externe du comportement suivant afin de définir correctement les attentes :

- La première fois qu'un utilisateur externe se connecte, le Firewall Threat Defense crée les structures requises mais ne peut pas créer simultanément la séance de l'utilisateur. L'utilisateur doit simplement s'authentifier à nouveau pour démarrer la session. L'utilisateur verra un message semblable au suivant : « New external username identified. Please log in again to start a session. » (Vos privilèges d'autorisation ont changé. Veuillez vous reconnecter pour lancer une session.)
- De même, si l'autorisation de l'utilisateur (définie dans le type de service) a été modifiée depuis la dernière connexion, l'utilisateur devra s'authentifier de nouveau. L'utilisateur verra un message semblable

au suivant : « Your authorization privilege has changed. Please log in again to start a session. » (Vos privilèges d'autorisation ont changé. Veuillez vous reconnecter pour lancer une session.)

Si des utilisateurs externes peuvent se connecter à l'interface graphique, mais pas à l'interface de commande en ligne, il pourrait y avoir un problème de clé secrète pour les serveurs AAA. Assurez-vous que les clés ne comprennent pas les caractères & ou \. Bien que ceux-ci puissent fonctionner avec les connexions à l'interface graphique utilisateur, ils ne fonctionnent pas avec les connexions SSH.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis cliquez sur le lien**System Settings** > **Management Access**.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **Management Access List** (liste d'accès de gestion) dans la table des matières.

Étape 2 Cliquez sur l'onglet **AAA Configuration** s'il n'est pas déjà sélectionné.

Étape 3 Configurez les options de connexion SSH (**SSH Connection**) :

- **Server Group** (groupe de serveurs) : Sélectionnez le groupe de serveurs RADIUS ou la base de données d'utilisateurs locaux (LocalIdentitySource) que vous souhaitez utiliser comme source d'authentification principale. Vous devez sélectionner un groupe de serveurs RADIUS pour utiliser une autorisation externe.

  Si le groupe de serveurs n'existe pas encore, cliquez sur le lien **Create New RADIUS Server Group** pour créer immédiatement un nouveau groupe de serveurs RADIUS. Vous devrez également créer des objets de serveur RADIUS pour chaque serveur, afin de les ajouter au groupe, mais vous pouvez le faire tout en définissant le groupe de serveurs. Pour en savoir plus sur RADIUS, consultez Serveurs et groupes RADIUS, à la page 176.

  Notez que les connexions SSH utilisent uniquement les deux premiers serveurs du groupe. Si vous utilisez un groupe comptant trois serveurs ou plus, les serveurs supplémentaires ne seront jamais essayés. En outre, les attributs de groupe **Dead Time** (temps mort) et **Maximum Failed Attempts** (nombre maximal de tentatives échouées) ne sont pas utilisés.

- **Authentification with LOCAL** : Si vous sélectionnez un groupe de serveurs externes, vous pouvez spécifier comment utiliser la source d'identité locale. Pour l'accès SSH, la base de données locale est toujours vérifiée avant le serveur externe.

Étape 4 Cliquez sur **Save** (Enregistrer).

Gérer les sessions des utilisateurs Gestionnaire de périphériques de pare-feu

Choisissez **Monitoring (Surveillance)** > **Sessions** pour afficher la liste des utilisateurs actuellement connectés à Gestionnaire de périphériques de pare-feu. La liste indique la durée de connexion de chaque utilisateur pour la session actuelle.

Si le même nom d'utilisateur apparaît plus d'une fois, cela signifie que l'utilisateur a ouvert des sessions à partir d'adresses source différentes. Les sessions sont suivies séparément en fonction du nom d'utilisateur et de l'adresse source, chaque session ayant son propre horodatage unique.

Le système permet 5 sessions utilisateur simultanées. Si un sixième utilisateur se connecte, la session utilisateur la plus ancienne est automatiquement déconnectée. En outre, les utilisateurs inactifs sont automatiquement déconnectés après 20 minutes d'inactivité.

Si l'utilisateur Gestionnaire de périphériques de pare-feu saisit le mauvais mot de passe et ne parvient pas à se connecter lors de 3 tentatives consécutives, le compte de l'utilisateur est verrouillé pendant 5 minutes. L'utilisateur doit attendre avant de réessayer de se connecter. Il n'y a aucun moyen de déverrouiller le compte d'utilisateur Gestionnaire de périphériques de pare-feu, ni d'ajuster le nombre de tentatives ou le délai de verrouillage. (Notez que pour les utilisateurs SSH, vous pouvez ajuster ces paramètres et déverrouiller le compte.)

Si nécessaire, vous pouvez mettre fin à une session utilisateur en cliquant sur l'icône de suppression ( ) de la session. Si vous supprimez votre propre session, vous êtes également déconnecté. Il n'y a pas de période de verrouillage si vous mettez fin à une session : l'utilisateur peut se connecter immédiatement.

Activation de l'accès Gestionnaire de périphériques de pare-feu sur une unité de secours à haute disponibilité pour les utilisateurs externes

Si vous configurez l'autorisation extérieure pour les utilisateurs Gestionnaire de périphériques de pare-feu, ces utilisateurs peuvent se connecter à l'unité active et en veille d'une paire à haute disponibilité. Cependant, la connexion réussie à l'unité de secours pour la première fois nécessite quelques étapes supplémentaires par rapport à la connexion à l'unité active.

Après qu'un utilisateur externe se soit connecté à l'unité active pour la première fois, le système crée un objet qui définit l'utilisateur et les droits d'accès de l'utilisateur. Un utilisateur administrateur ou en lecture-écriture doit ensuite déployer la configuration à partir de l'unité active pour que l'objet utilisateur s'affiche sur l'unité de secours.

Ce n'est qu'après l'achèvement réussi du déploiement et de la synchronisation de la configuration que l'utilisateur externe peut se connecter à l'unité de secours.

Les utilisateurs administrateurs et de lecture-écriture peuvent déployer les modifications après s'être connectés à l'unité active. Cependant, les utilisateurs en lecture seule ne peuvent pas déployer la configuration et doivent demander à un utilisateur disposant des droits appropriés de déployer la configuration.

Création de comptes d'utilisateur locaux pour l'interface de ligne de commande de Firewall Threat Defense

Vous pouvez créer des utilisateurs pour l'accès à l'interface de ligne de commande sur les appareils Firepower Threat Defense. Ces comptes ne permettent pas l'accès à l'application de gestion, mais à l'interface de ligne de commande uniquement. L'interface de ligne de commande est utile pour le dépannage et la surveillance.

Vous ne pouvez pas créer de comptes utilisateur locaux sur plusieurs appareils à la fois. Chaque périphérique possède son propre ensemble de comptes utilisateur uniques d'interface de ligne de commande.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande de l'appareil en utilisant un compte avec des privilèges de configuration.

Le compte d'utilisateur admin dispose des privilèges requis, mais tout compte doté de privilèges de configuration fonctionnera. Vous pouvez utiliser une session SSH ou le port de console.

Pour certains modèles d'appareils, le port de console vous place dans l'interface de ligne de commande FXOS. Utilisez la commande **connect ftd** pour accéder à l'interface de ligne de commande Firepower Threat Defense.

Étape 2 Créez un compte utilisateur.

configure user add *username* (nom d'utilisateur) {**basic** | **config**}

Vous pouvez définir l'utilisateur avec les niveaux de privilège suivants :

- **config** : Donne accès à la configuration utilisateur. Cela donne à l'utilisateur tous les droits d'administrateur sur toutes les commandes.
- **basic** : Donne à l'utilisateur un accès de base. Cela ne permet pas à l'utilisateur d'entrer des commandes de configuration.

Exemple :

Dans l'exemple suivant, un compte d'utilisateur nommé joecool est ajouté avec des droits d'accès de configuration. Le mot de passe ne s'affiche pas lorsque vous le saisissez.

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

Remarque
L'utilisateur est invité à changer le mot de passe lors de la première connexion. L'utilisateur peut initier des modifications de mot de passe ultérieures à l'aide de la commande **configure password**.

Étape 3 (Facultatif) Ajustez les caractéristiques du compte pour satisfaire à vos exigences de sécurité.

Vous pouvez utiliser les commandes suivantes pour modifier le comportement par défaut du compte.

- **configure user aging** *nom d'utilisateur max_days warn_days*

  Définit une date d'expiration pour le mot de passe de l'utilisateur. Précisez le nombre maximal de jours de la période de validité du mot de passe, suivi du nombre de jours de préavis (c.-à-d. le moment auquel l'utilisateur sera averti de l'expiration prochaine). Les deux valeurs sont comprises entre 1 et 9999, mais le nombre de jours de préavis doit être inférieur au nombre de jours de la période de validité maximale. Lorsque vous créez le compte, le mot de passe ne comporte aucune date d'échéance.

- **configure user forcereset** *username (nom d'utilisateur)*

  Force l'utilisateur à modifier le mot de passe lors de la prochaine connexion.

- **configure user maxfailedlogins** *username number (numéro d'utilisateur)*

  Définit le nombre maximal de connexions échouées consécutives que vous autoriserez avant de verrouiller le compte (de 1 à 9999). Utilisez la commande **configure user unlock** pour déverrouiller des comptes. La valeur par défaut pour les nouveaux comptes est cinq échecs consécutifs de connexion.

- **configure user minpasswdlen** *username number (numéro d'utilisateur)*

Définit une longueur de mot de passe minimale, qui peut aller de 1 à 127.

- **configure user strengthcheck** *username (nom d'utilisateur)* {**enable** | **disable**}

  Active ou désactive la vérification de la force du mot de passe, qui contraint un utilisateur à répondre à des critères de mot de passe spécifiques lors de la modification de son mot de passe. Lorsque le mot de passe d'un utilisateur expire ou si la commande **configure user forcereset** est utilisée, cette exigence est automatiquement activée lors de la prochaine connexion de l'utilisateur.

Étape 4 Gérez les comptes utilisateur au besoin.

Il arrive que des comptes soient verrouillés ou que vous deviez supprimer des comptes ou résoudre d'autres problèmes. Utilisez les commandes suivantes pour gérer les comptes d'utilisateur dans le système.

- **configure user access** *username (nom d'utilisateur)* {**basic** | **config**}

  Modifie les privilèges d'un compte d'utilisateur.

- **configure user delete** *username (nom d'utilisateur)*

  Supprime le compte spécifié.

- **configure user disable** *username (nom d'utilisateur)*

  Désactive le compte spécifié sans le supprimer. L'utilisateur ne peut pas se connecter tant que vous n'avez pas activé le compte.

- **configure user enable** *username (nom d'utilisateur)*

  Active le compte spécifié.

- **configure user password** *username (nom d'utilisateur)*

  Modifie le mot de passe de l'utilisateur spécifié. Les utilisateurs doivent normalement modifier leur propre mot de passe à l'aide de la commande **configure password**.

- **configure user unlock** *username (nom d'utilisateur)*

  Déverrouille un compte d'utilisateur qui a été verrouillé en raison du nombre maximal de tentatives de connexion échouées consécutives.

Redémarrage ou arrêt du système

Si nécessaire, vous pouvez redémarrer ou arrêter le système.

En plus de la procédure ci-dessous, vous pouvez également effectuer ces tâches par le biais d'une session SSH ou de la console CLI Gestionnaire de périphériques de pare-feu en utilisant les commandes **reboot** ou **shutdown**.

Remarque L'ISA 3000 ne prend pas en charge l'arrêt; vous pouvez uniquement redémarrer le système.

Procédure

Étape 1 Cliquez sur **Device** (périphérique), puis cliquez sur le lien **System Settings (paramètres système)** > **Reboot/Shutdown (redémarrage/arrêt)**.

Si vous êtes déjà dans la page des paramètres système, cliquez simplement sur **Reboot/Shutdown** (redémarrage/arrêt) dans la table des matières.

Étape 2 Cliquez sur le bouton qui effectue la fonction dont vous avez besoin.

- **Reboot** (Redémarrer) : si vous pensez que le système ne fonctionne pas correctement et que d'autres tentatives pour résoudre le problème ont échoué, vous pouvez redémarrer le périphérique. En outre, il peut y avoir quelques procédures qui vous demanderont de redémarrer le périphérique pour recharger le logiciel système.
- **Reboot** (Redémarrer) : mettez le système hors tension de manière contrôlée. Utilisez l'arrêt lorsque vous avez l'intention de retirer le périphérique du réseau, par exemple pour le remplacer. Après avoir éteint le périphérique, vous pouvez le rallumer uniquement à partir du commutateur marche/arrêt du matériel.

Étape 3 Attendez que l'action soit terminée.

Si vous disposez d'une connexion de console au pare-feu, surveillez les notifications du système lorsque le pare-feu s'éteint. La notification suivante s'affichera :

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Vous ne pouvez pas effectuer d'autres actions dans Gestionnaire de périphériques de pare-feu ou l'interface de ligne de commande pendant le redémarrage ou l'arrêt du système.

Pendant le redémarrage, la page Gestionnaire de périphériques de pare-feu devrait être actualisée une fois le redémarrage terminé et vous mener à la page de connexion. Si vous essayez d'actualiser la page avant la fin du redémarrage, le navigateur Web peut renvoyer des erreurs 503 ou 404, en fonction de l'état opérationnel du serveur Web Gestionnaire de périphériques de pare-feu à ce moment-là.

Pour l'arrêt, le système ne pourra pas répondre du tout et vous obtiendrez des erreurs 404. Il s'agit du résultat attendu, car vous éteignez complètement le système.

Dépannage du système

Les rubriques suivantes traitent de certaines tâches et fonctionnalités de résolution de problèmes au niveau du système. Pour en savoir plus sur le dépannage d'une fonction en particulier, comme le contrôle d'accès, consultez le chapitre correspondant.

Envoi de requêtes ping pour tester la connectivité

La commande ping est un outil simple qui vous permet de déterminer si une adresse particulière est active et répond. Cela signifie que la connectivité de base fonctionne. Cependant, d'autres politiques exécutées sur un

périphérique peuvent empêcher des types de trafic spécifiques de passer par un périphérique. Vous pouvez l'utiliser **ping** en ouvrant la console d'interface de ligne de commande ou en vous connectant à l'interface de ligne de commande du périphérique.



Remarque Comme le système dispose de plusieurs interfaces, vous pouvez contrôler l'interface utilisée pour envoyer un ping à une adresse. Vous devez vous assurer que vous utilisez la bonne commande, afin de tester la connectivité qui compte. Par exemple, le système doit pouvoir atteindre le serveur de licences Cisco par l'intermédiaire de l'interface de gestion virtuelle . Vous devez donc utiliser la commande **ping system** pour tester la connexion. Si vous utilisez **ping**, vous testez si une adresse peut être atteinte par l'intermédiaire des interfaces de données, ce qui pourrait ne pas vous donner le même résultat.

Le ping normal utilise des paquets ICMP pour tester la connexion. Si votre réseau interdit ICMP, vous pouvez utiliser un ping TCP à la place (pour les pings d'interface de données uniquement).

Vous pouvez envoyer un ping à une adresse IP ou à un nom de domaine complet (FQDN). Pour qu'un ping fonctionne sur un nom de domaine complet, les serveurs DNS configurés pour les interfaces de gestion ou de données doivent renvoyer avec succès une adresse IP. Vous devez configurer séparément les serveurs DNS pour les interfaces de gestion et de données. Si vous n'avez pas configuré de serveurs DNS pour une interface spécifique, utilisez la commande **nslookup** *fqdn-name* pour rechercher l'adresse IP d'un nom de domaine complet donné.

Voici les principales options pour envoyer des pings aux adresses réseau.

Ping d'une adresse par l'intermédiaire de l'interface de gestion virtuelle

Utilisez la commande **ping system**.

ping system *host*

L'hôte peut être une adresse IP ou un nom de domaine complet (FQDN), tel que www.exemple.com. Contrairement aux pings via les interfaces de données, il n'y a pas de nombre par défaut pour les pings système. Le ping continue jusqu'à ce que vous l'arrêtiez à l'aide de Ctrl+C. Par exemple :

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

Ping d'une adresse par l'intermédiaire d'une interface de données à l'aide de la table de routage

Utilisez la commande **ping**. Sans préciser d'interface, vous testez si le système peut trouver de manière générique une voie de routage vers l'hôte. Comme il s'agit de la façon dont le système achemine normalement le trafic, c'est généralement ce que vous souhaitez tester.

ping *host*

Par exemple :

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Remarque Vous pouvez préciser le délai d'expiration, le nombre de répétitions, la taille des paquets et même le modèle de données à envoyer. Utilisez l'indicateur d'aide « ? » dans la console d'interface en ligne de commande pour voir les options disponibles.

Ping d'une adresse par l'intermédiaire d'une interface de données spécifique

Utilisez la commande **ping interface** *if_name* si vous souhaitez tester la connectivité par l'intermédiaire d'une interface de données spécifique. Vous pouvez également spécifier l'interface de diagnostic en utilisant cette commande, mais pas l'interface de gestion virtuelle.

ping interface *if_name hôte*

Par exemple :

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Ping d'une adresse par l'intermédiaire d'une interface de données à l'aide du ping TCP

Utilisez la commande **ping tcp**. Un ping TCP envoie des paquets SYN et considère l'envoi ping comme réussi si la destination envoie un paquet SYN-ACK.

ping tcp [**interface** *if_name*] *hôte port*

Vous devez préciser l'hôte et le port TCP.

Vous pouvez éventuellement préciser l'interface, qui est l'interface source du ping, et non l'interface par laquelle envoyer les ping. Ce type de ping utilise toujours la table de routage.

Un ping TCP envoie des paquets SYN et considère l'envoi ping comme réussi si la destination envoie un paquet SYN-ACK. Par exemple :

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Remarque Vous pouvez également préciser le délai d'expiration, le nombre de répétitions et l'adresse source du ping TCP. Utilisez l'indicateur d'aide, ?, dans l'interface de ligne de commande pour voir les options disponibles.

Suivi des routes vers les hôtes

Si vous éprouvez des problèmes pour envoyer le trafic vers une adresse IP, vous pouvez retracer la route vers l'hôte pour déterminer s'il y a un problème sur le chemin du réseau. Un traceroute fonctionne par envoi de paquets UDP sur un port non valide, ou d'échos ICMPv6, vers une destination. Les routeurs le long du chemin vers la destination répondent avec un message ICMP Time Exceeded et signalent cette erreur à traceroute. Chaque nœud reçoit trois paquets, ce qui vous donne trois possibilités par nœud d'obtenir un résultat informatif. Vous pouvez l'utiliser **traceroute** en ouvrant la console d'interface de ligne de commande ou en vous connectant à l'interface de ligne de commande du périphérique.



Remarque Il existe des commandes distinctes pour tracer un routage par l'intermédiaire d'une interface de données (**traceroute**) ou par l'interface de gestion virtuelle (**traceroute system**). Assurez-vous d'utiliser la bonne commande.

Le tableau suivant décrit le résultat possible par paquet, comme affiché dans la sortie.

Symbole de sortie	Description
*	Aucune réponse n'a été reçue pour la sonde dans le délai d'expiration.
nn msec	Pour chaque nœud, le temps d'aller-retour (en millisecondes) pour le nombre spécifié de sondes.
!N.	Réseau ICMP inaccessible.
!H	Hôte ICMP inaccessible.
!P	Protocole inaccessible ICMP
!A	ICMP administrativement interdit.
?	Erreur ICMP inconnue.

Suivi d'un routage par le biais de l'interface de gestion virtuelle

Utilisez la commande **traceroute system**.

traceroute system *destination*

L'hôte peut être une adresse IPv4/IPv6 ou un nom de domaine complet (FQDN), tel que www.exemple.com. Par exemple :

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
```

```
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

Suivi d'un routage par le biais d'une interface de données

Utilisez la commande **traceroute**.

traceroute *destination*

L'hôte peut être une adresse IPv4 ou IPv6 ou un nom de domaine complet (FQDN), tel que www.exemple.com, si vous configurez les serveurs DNS pour les interfaces de données. Si vous n'avez pas configuré de serveurs DNS pour une interface spécifique, utilisez la commande **nslookup** *fqdn-name* pour rechercher l'adresse IP d'un nom de domaine complet donné. Par exemple :

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

Remarque Vous pouvez préciser le délai d'expiration, la durée de vie, le nombre de paquets par nœud et même l'adresse IP ou l'interface à utiliser comme source du traceroute. Utilisez l'indicateur d'aide, ?, dans l'interface de ligne de commande pour voir les options disponibles.

Faire apparaître le périphérique sur les Traceroutes

Par défaut, le périphérique Firewall Threat Defense n'apparaît pas sur les Traceroutes en tant que saut. Pour l'afficher, vous devez décrémenter la durée de vie des paquets qui passent par le périphérique et augmenter la limite de débit pour les messages ICMP unreachable. Pour ce faire, vous devez créer un objet FlexConfig qui configure la règle de politique de service requise et d'autres options.

Pour une description détaillée des politiques de service et des classes de trafic, consultez le *guide de configuration des pare-feu Cisco ASA Series* accessible à l'adresse https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html.

Remarque Si vous décrémentez la durée de vie, les paquets avec une TTL de 1 seront abandonnés, mais une connexion sera ouverte pour la session en supposant que la connexion pourrait contenir des paquets avec une TTL plus élevée. Notez que certains paquets, comme les paquets Hello d'OSPF, sont envoyés avec une TTL = 1, donc la décrémentation de la durée de vie peut avoir des conséquences inattendues. Gardez ces considérations à l'esprit lorsque vous définissez votre classe de trafic.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Créez l'objet pour décrémenter le TTL.

a) Cliquez sur le bouton **+** pour créer un nouvel objet.

b) Saisissez un nom pour l'objet. Par exemple, **Décrémenter_TTL**.

c) Dans l'éditeur **Template** (Modèle), saisissez les lignes suivantes, y compris les indentations.

```
icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  set connection decrement-ttl
```

d) Dans l'éditeur **Negate Template** (Modèle d'annulation), saisissez les lignes nécessaires pour annuler cette configuration.

Tout comme vous devez inclure les commandes parentes pour entrer dans le sous-mode approprié pour une commande afin de l'activer, vous devez également inclure ces commandes dans le modèle de négation.

Le modèle d'annulation sera appliqué si vous supprimez cet objet de la politique FlexConfig (après l'avoir déployé avec succès), et également lors d'un déploiement infructueux (pour réinitialiser la configuration à son état précédent).

Ainsi, pour cet exemple, le modèle de négation serait le suivant :

```
no icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  no set connection decrement-ttl
```

e) Cliquez sur **OK** pour enregistrer l'objet.

Étape 4 Ajoutez les objets à la politique FlexConfig.

Seuls les objets sélectionnés dans la politique FlexConfig sont déployés.

a) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières.

b) Cliquez sur **+** dans la liste des groupes.

c) Sélectionnez l'objet Dement_TTL et cliquez sur **OK**.

L'aperçu doit être mis à jour avec les commandes du modèle. Vérifiez que vous voyez les commandes attendues.

d) Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant déployer la politique.

Dépannage du protocole NTP

Le système dépend d'une heure précise et constante pour fonctionner correctement et pour s'assurer que les événements et les autres points de données sont traités avec exactitude. Vous devez configurer au moins un, mais idéalement trois, serveurs NTP (Network Time Protocol) pour que le système dispose toujours d'informations horaires fiables.

Le diagramme récapitulatif de la connexion du périphérique (cliquez sur **Device** (Périphérique) dans le menu principal) affiche l'état de la connexion au serveur NTP. Si l'état est jaune ou orange, un problème de connexion existe avec les serveurs configurés. Si le problème de connexion persiste (et qu'il ne s'agit pas simplement d'un problème momentané), essayez ce qui suit.

- Tout d'abord, assurez-vous qu'au moins trois serveurs NTP sont configurés dans **Device (Périphérique)** > **System Settings (Paramètres système)** > **NTP**. Bien qu'il ne s'agisse pas d'une exigence, la fiabilité est considérablement améliorée si vous avez au moins trois serveurs NTP.
- Assurez-vous qu'il existe un chemin réseau entre l'adresse IP de l'interface de gestion (définie dans **Device (Périphérique)** > **System Settings (Paramètres système)** > **Management Interface (Interface de gestion)**) et les serveurs NTP.
  - Si la passerelle de l'interface de gestion correspond aux interfaces de données, vous pouvez configurer des routes statiques vers les serveurs NTP dans **Device (Périphérique)** > **Routing (Routage)** si la route par défaut n'est pas adéquate.
  - Si vous définissez une passerelle d'interface de gestion explicite, connectez-vous à l'interface CLI du périphérique et utilisez la commande **ping system** pour vérifier s'il existe un chemin réseau vers chaque serveur NTP.
- Connectez-vous à l'interface CLI du périphérique et vérifiez l'état des serveurs NTP à l'aide des commandes suivantes.
  - **show ntp** : cette commande affiche des informations de base sur les serveurs NTP et leur disponibilité. Cependant, l'état de connectivité dans le Gestionnaire de périphériques de pare-feu utilise des informations supplémentaires pour indiquer l'état, de sorte qu'il peut y avoir une incohérence dans ce que cette commande affiche et ce que montre le diagramme d'état de connectivité. Vous pouvez également émettre cette commande à partir de la console d'interface de ligne de commande.
  - **system support ntp** : cette commande comprend la sortie de **show ntp** plus la sortie de la commande NTP standard **ntpq**, qui est documentée avec le protocole NTP. Utilisez cette commande si vous devez confirmer la synchronisation NTP.

    Recherchez la section « Résultats de « ntpq -pn ». Par exemple, vous pourriez voir quelque chose comme ce qui suit :

```
Results of 'ntpq -pn'
remote                    : +216.229.0.50
refid                     : 129.7.1.66
st                        : 2
t                         : u
when                      : 704
poll                      : 1024
reach                     : 377
delay                     : 90.455
offset                    : 2.954
jitter                    : 2.473
```

Dans cet exemple, le signe plus (+) avant l'adresse du serveur NTP indique qu'il s'agit d'un candidat potentiel. Un astérisque ici, *, indique l'homologue de la source de temps actuelle.

Le démon NTP (NTPD) utilise une fenêtre glissante de huit échantillons pour chacun des homologues et en sélectionne un, puis la sélection de l'horloge détermine les vraies sources et les fausses. NTPD détermine ensuite la distance aller-retour (le décalage d'un candidat ne doit pas dépasser la moitié du retard aller-retour). Si des retards de connexion, une perte de paquets ou des problèmes de serveur entraînent le rejet d'un ou de tous les candidats, vous verrez de longs retards dans la synchronisation. L'ajustement se produit également sur une très longue période : les erreurs de décalage d'horloge et d'oscillateur doivent être résolues par l'algorithme de correction d'horloge, ce qui peut prendre des heures.

Remarque Si le refid est .LOCL., cela indique que l'homologue est une horloge locale non asservie, c'est-à-dire qu'il utilise son horloge locale uniquement pour définir l'heure. Le Gestionnaire de périphériques de pare-feu marque toujours la connexion NTP en jaune (non synchronisée) si l'homologue sélectionné est .LOCL. Normalement, le protocole NTP ne sélectionne pas un candidat .LOCL. si un meilleur est disponible, c'est pourquoi vous devez configurer au moins trois serveurs.

Dépannage du DNS pour l'interface de gestion

Vous devez configurer au moins un serveur DNS pour l'utilisation par l'interface de gestion. Le serveur est nécessaire pour les connexions en nuage aux services tels que les licences Smart, les mises à jour de bases de données (comme GeoDB, règles et VDB) et toute autre activité nécessitant une résolution du nom de domaine.

La configuration d'un serveur DNS est plutôt simple. Il suffit d'entrer les adresses IP des serveurs DNS que vous utilisez lors de la configuration initiale de l'appareil. Vous pourrez les modifier ultérieurement dans la page **Device (périphérique)** > **System Settings (paramètres système)** > **DNS Server (serveur DNS)**.

Cependant, le système peut ne pas résoudre les noms de domaine complets (FQDN) en raison de problèmes de connectivité réseau ou du serveur DNS lui-même. Si vous constatez que le système ne peut pas utiliser vos serveurs DNS, envisagez les actions suivantes pour cerner et résoudre le problème. Vous pouvez aussi consulter Dépannage des problèmes généraux de DNS, à la page 800.

Procédure

Étape 1 Déterminez si vous avez un problème.

a) Utilisez SSH pour vous connecter à l'interface de ligne de commande de l'appareil.

b) Entrez **ping system www.cisco.com**. Si vous obtenez un message « unknown host » (hôte inconnu) comme le suivant, le système ne pourra pas résoudre le nom de domaine. Si le message ping réussit, alors vous avez terminé : le DNS fonctionne. (Appuyez sur Ctrl + C pour arrêter le message ping.)

```
> ping system www.cisco.com
ping: unknown host www.cisco.com
```

Remarque
Il est essentiel d'inclure le mot clé **system** dans la commande **ping**. Le mot clé **system** envoie le message ping via l'adresse IP de gestion, qui est la seule interface qui utilise le serveur DNS de gestion. L'envoi d'un message ping www.cisco.com est également une bonne option, car vous avez besoin d'une voie de routage vers ce serveur pour les licences Smart et les mises à jour.

Étape 2 Vérifiez la configuration de l'interface de gestion.

a) Cliquez sur **Device (périphérique)** > **System Settings (paramètres système)** > **Management Interface (interface de gestion)**, puis vérifiez les points suivants. Si vous apportez des modifications, les modifications sont appliquées immédiatement lorsque vous cliquez sur **Save** (enregistrer). Si vous modifiez l'adresse de gestion, vous devrez vous reconnecter et ouvrir une nouvelle session.

- L'adresse IP de la passerelle est correcte pour le réseau de gestion. Si vous utilisez les interfaces de données comme passerelle, les étapes suivantes vérifieront cette configuration.
- Si vous n'utilisez pas les interfaces de données comme passerelle, vérifiez que l'adresse IP de gestion (ou le masque de sous-réseau) et l'adresse IP de la passerelle se trouvent sur le même sous-réseau.

b) Cliquez sur **Device (périphérique)** > **System Settings (paramètres système)** > **DNS Server (serveur DNS)** et vérifiez que les bons serveurs DNS sont configurés.

Si vous déployez le périphérique sur votre périphérie réseau, votre fournisseur de services peut avoir des exigences spécifiques concernant le serveur DNS que vous pouvez utiliser.

c) Si vous utilisez les interfaces de données comme passerelle, vérifiez que vous disposez des voies de routage requises.

Vous avez besoin d'une voie de routage par défaut pour 0.0.0.0. Vous pourriez avoir besoin de voies de routage supplémentaire si le serveur DNS n'est pas disponible par la passerelle pour le routage par défaut. Fondamentalement, il y a deux types de situations :

- Si vous utilisez DHCP pour obtenir une adresse pour l'interface extérieure, et que vous avez sélectionné l'option **Obtain Default Route using DHCP (obtenir la route par défaut à l'aide de DHCP)**, la route par défaut n'est pas visible dans le Gestionnaire de périphériques de pare-feu. À partir de SSH, entrez **show route** et vérifiez qu'il existe une voie de routage pour 0.0.0.0. Puisque c'est la configuration par défaut pour l'interface externe, il s'agit d'une situation probable. (allez à **Device (appareil)** > **Interfaces interfaces)** pour voir la configuration de l'interface extérieure.)
- Si vous utilisez une adresse IP statique sur l'interface externe ou si vous n'obtenez pas la voie de routage par défaut de DHCP, ouvrez **Device (périphérique)** > **Routing (routage)**. Vérifiez que la bonne passerelle est utilisée pour la voie de routage par défaut.

Si le serveur DNS ne peut pas être atteint par la voie de routage par défaut, vous devez définir une voie de routage statique vers celui-ci sur la page **Routing** (routage). Notez que vous ne devez pas ajouter de voies de routage pour les réseaux directement connectés, c.-à-d. Les réseaux qui sont connectés directement à l'une des interfaces de données du système, car le système peut assurer le routage vers ces réseaux automatiquement.

Vérifiez également qu'il n'y a aucune voie de routage statique qui dirige le trafic vers le serveur par la mauvaise interface.

d) Si le bouton de déploiement indique des modifications non déployées, déployez-les maintenant et attendez la fin du déploiement.



e) Effectuez un nouveau test sur **ping system www.cisco.com**. Si vous rencontrez toujours des problèmes, passez à l'étape suivante.

Étape 3 Dans la session SSH, entrez **nslookup www.cisco.com**.

- Si **nslookup** indique qu'il a obtenu une réponse du serveur DNS, mais que le serveur n'a pas pu trouver le nom, cela signifie que DNS est configuré correctement, mais que le serveur DNS que vous utilisez n'a pas d'adresse pour le nom de domaine complet. La réponse ressemblerait à ceci :

```
> nslookup www.cisco.com
Server:         10.163.47.11
Address:        10.163.47.11#53

** server can't find www.cisco.com: NXDOMAIN
```

Résolution : Dans ce cas, vous devez configurer un serveur DNS différent ou obtenir celui que vous avez mis à jour pour qu'il puisse résoudre les noms de domaine complets dont vous avez besoin. Collaborez avec votre administrateur réseau ou votre fournisseur de services Internet pour obtenir l'adresse IP d'un serveur DNS qui fonctionnera pour votre réseau.

- Si vous recevez un message « connection timed out » (expiration de la connexion), cela signifie que le système ne peut pas atteindre vos serveurs DNS ou encore, que tous les serveurs DNS sont actuellement en panne et ne répondent pas (ce qui est moins probable). Passez à l'étape suivante.

```
> nslookup www.cisco.com
; ; connection timed out; no servers could be reached
```

Étape 4 Utilisez la commande **traceroute system** *DNS_server_ip_address* pour tracer la voie de routage vers le serveur DNS.

Par exemple, si le serveur DNS est 10.100.10.1, entrez :

```
> traceroute system 10.100.10.1
```

Voici les résultats possibles :

- L'opération traceroute s'achève en parvenant au serveur DNS. Dans ce cas, en fait, il y a une voie de routage vers le serveur DNS et le système peut l'atteindre. Ainsi, il n'y a aucun problème de routage. Cependant, pour une raison ou une autre, les demandes DNS vers ce serveur ne reçoivent pas de réponse.

  Résolution: il est possible qu'un routeur ou un pare-feu bloque le trafic UDP/53, qui est le port utilisé pour le DNS. Vous pouvez essayer un serveur DNS sur un chemin réseau différent. Il s'agit d'un problème difficile à résoudre, car vous devrez déterminer quel nœud bloque le trafic et travailler avec l'administrateur système pour modifier les règles d'accès.

- L'opération traceroute ne peut pas atteindre ne serait-ce qu'un seul nœud, ce qui ressemblerait à ceci :

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1  * * *
```

```
 2  * * *
 3  * * *
(and so forth)
```

Résolution : dans ce cas, le problème de routage est au niveau du système. Essayez de faire un **ping system** pour l'adresse IP de la passerelle. Revérifiez la configuration de l'interface de gestion comme indiqué dans les étapes précédentes et assurez-vous que les passerelles et les voies de routage requises sont configurées.

- L'opération traceroute traverse quelques nœuds avant de parvenir à un point où elle ne peut plus résoudre la voie de routage, ce qui ressemblerait à ceci :

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.475 ms  0.532 ms  0.542 ms
 2  10.88.127.1 (10.88.127.1)  0.803 ms  1.434 ms  1.443 ms
 3  site04-lab-gw1.example.com (10.89.128.25)  1.390 ms  1.399 ms  1.435 ms
 4  * * *
 5  * * *
 6  * * *
```

Résolution : Dans ce cas, le routage est interrompu au dernier nœud. Vous devrez peut-être travailler avec l'administrateur système pour obtenir l'installation des voies de routage correctes dans ce nœud. Cependant, s'il n'y a intentionnellement aucune voie de routage vers le serveur DNS par le biais du nœud, vous devez modifier votre passerelle ou créer votre propre voie de routage statique pour orienter le trafic vers un routeur qui peut l'acheminer jusqu'au serveur DNS.

Analyse de l'utilisation du processeur et de la mémoire

Pour afficher les informations au niveau du système concernant l'utilisation du processeur et de la mémoire, sélectionnez **Monitoring (Surveillance)** > **System (Système)** et recherchez les graphiques à barres du processeur et de la mémoire. Ces graphiques affichent les informations collectées par l'interface de ligne de commande à l'aide des commandes **show cpu system** et **show memory system**.

Si vous ouvrez la console d'interface de ligne de commande ou vous connectez à celle-ci, vous pouvez utiliser des versions supplémentaires de ces commandes pour afficher d'autres informations. En règle générale, vous ne consulterez ces renseignements que si vous avez des problèmes persistants d'utilisation ou sous la demande du centre d'assistance technique de Cisco (TAC). Une grande partie des renseignements détaillés sont complexes et nécessitent une explication par le TAC.

Voici quelques points saillants de ce que vous pouvez examiner. Vous pouvez trouver des informations plus détaillées sur ces commandes dans Référence de commande Cisco Firepower Threat Defense à l'adresse http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.

- **show cpu** affiche l'utilisation du processeur du plan de données.
- **show cpu core** affiche l'utilisation de chaque cœur de CPU séparément.
- **show cpu detailed** affiche l'utilisation supplémentaire de la CPU par cœur et globale du plan de données.
- **show memory** affiche l'utilisation de la mémoire du plan de données.

Remarque Certains mots-clés (non mentionnés ci-dessus) nécessitent que vous configuriez d'abord le profilage ou d'autres fonctionnalités à l'aide des commandes **cpu** ou **memory**. Utilisez ces fonctionnalités uniquement selon les directives du TAC.

Afficher les journaux des événements

Le système consigne les informations pour une grande variété d'actions. Vous pouvez utiliser la commande **system support view-files** pour ouvrir un journal système. Utilisez cette commande lorsque vous travaillez avec le centre d'assistance technique de Cisco (TAC) afin qu'il puisse vous aider à interpréter le résultat et pour sélectionner le journal approprié à afficher.

La commande présente un menu pour sélectionner un journal. Utilisez les commandes suivantes pour naviguer dans l'assistant :

- Pour passer à un sous-répertoire, saisissez le nom du répertoire et appuyez sur Enter (Entrée).
- Pour sélectionner un fichier à afficher, saisissez **s** à l'invite. Vous êtes invité à saisir un nom. Vous devez saisir le nom complet, en respectant la casse. La liste des fichiers vous indique la taille du journal, que vous pouvez prendre en compte avant d'ouvrir des journaux très volumineux.
- Appuyez sur la barre d'espace lorsque vous voyez --More (Plus)-- pour afficher la page suivante d'entrées de journal ; appuyez sur Enter (Entrée) pour n'afficher que l'entrée suivante. Lorsque vous atteignez la fin du journal, vous accédez au menu principal. La ligne --Plus-- vous affiche la taille du journal et la partie que vous avez affichée. **Utilisez les touches Ctrl + C pour fermer le journal et quitter la commande si vous ne souhaitez pas effectuer de page dans l'ensemble du journal.**
- Tapez **b** pour monter d'un niveau dans la structure jusqu'au menu.

Si vous souhaitez laisser le journal ouvert afin de pouvoir voir les nouveaux messages à mesure qu'ils sont ajoutés, utilisez la commande **tail-logs** au lieu de **system support view-files**.

L'exemple suivant montre comment afficher le fichier cisco/audit.log, qui suit les tentatives de connexion au système. La liste des fichiers commence par les répertoires en haut, puis une liste de fichiers dans le répertoire actuel.

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
```

```
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>


([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

============================
Directory: /ngfw/var/log/cisco
-----------files------------
2017-02-13 22:44:42.394907 | 472        | audit.log
2017-02-13 23:40:30.858198 | 903615     | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0          | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338    | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338    | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218    | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848      | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160    | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login successful,

2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked account.,


<remaining log truncated>
```

Création d'un fichier de dépannage

Le personnel du centre d'assistance technique de Cisco (TAC) peut vous demander de fournir des informations sur le journal du système lorsque vous soumettez un rapport de problème. Ces renseignements les aident à diagnostiquer le problème. Vous n'avez pas besoin d'envoyer de fichier de diagnostic, sauf si vous y êtes invité.

La procédure suivante explique comment créer et télécharger le fichier de diagnostic.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Sous **Troubleshooting** (Dépannage), cliquez sur **Request File to be Created** (Demander la création du fichier) ou **Re-Request File to be Created** (Redemander la création du fichier) (si vous en avez créé un auparavant).

Le système commence à générer le fichier de diagnostic. Vous pouvez accéder à d'autres pages et revenir ici pour vérifier l'état. Lorsque le fichier est prêt, la date et l'heure de la création du fichier s'affichent ainsi qu'un bouton de téléchargement.

Étape 3 Lorsque le fichier est prêt, cliquez sur le bouton de téléchargement.

Le fichier est téléchargé sur votre ordinateur à l'aide de la méthode de téléchargement standard de votre navigateur.

Basculement entre la gestion locale et la gestion à distance

Vous pouvez configurer et gérer votre périphérique à l'aide du gestionnaire local Gestionnaire de périphériques de pare-feu, qui est hébergé directement sur le périphérique, ou à distance, à l'aide du gestionnaire de périphériques multiples Centre de gestion Firepower (FMC). Vous pouvez utiliser le gestionnaire à distance si vous souhaitez configurer des fonctionnalités non prises en charge par Gestionnaire de périphériques de pare-feu, ou si vous avez besoin de la puissance et des capacités d'analyse offertes par Centre de gestion Firepower (FMC).

Vous devez également utiliser le Centre de gestion Firepower (FMC) si vous voulez exécuter le périphérique en mode de pare-feu transparent.

Vous pouvez basculer entre la gestion locale et la gestion à distance sans réinstaller le logiciel. Avant de passer de la gestion à distance à la gestion locale, vérifiez que le Gestionnaire de périphériques de pare-feu répond à toutes vos exigences de configuration.

⚠

Mise en garde Le passage à un autre gestionnaire efface la configuration du périphérique et ramène le système à la configuration par défaut. Cependant, l'adresse IP de gestion et le nom d'hôte sont conservés.

Avant de commencer

Si vous avez enregistré le périphérique, surtout si vous avez activé des licences de fonctionnalités, vous devez annuler l'enregistrement du périphérique par l'intermédiaire de Gestionnaire de périphériques de pare-feu avant de passer à la gestion à distance. La désinscription du périphérique libère la licence de base et toutes les licences de fonctionnalités. Si vous ne désinscrivez pas le périphérique, ces licences restent affectées au périphérique dans Cisco Smart Software Manager. Consultez Désinscrire le périphérique, à la page 97.

Si le périphérique est configuré pour la haute disponibilité, vous devez d'abord rompre la configuration de haute disponibilité à l'aide du gestionnaire de périphériques (si possible) ou de la commande **configure high-availability disable**. Idéalement, interrompez la haute disponibilité à partir de l'unité active.

Procédure

Étape 1 Utilisez un client SSH pour ouvrir une connexion à **l'adresse IP de gestion** et vous connecter à l'interface de ligne de commande du périphérique avec un nom d'utilisateur qui dispose d'un accès à l'interface de ligne de commande de configuration. Par exemple, le nom d'utilisateur **admin**.

Il est important que vous suiviez ce processus lorsque vous êtes connecté à l'adresse IP de gestion. Lorsque vous utilisez Gestionnaire de périphériques de pare-feu, vous avez la possibilité de gérer le périphérique au moyen de l'adresse IP d'une interface de données. Cependant, vous devez utiliser le port physique de gestion et l'adresse IP de gestion pour administrer le périphérique à distance.

Si vous ne pouvez pas vous connecter à l'adresse IP de gestion, adressez-vous aux points suivants :

- Vérifiez que le port physique de gestion est câblé à un réseau fonctionnel.
- Assurez-vous que l'adresse IP de gestion et la passerelle sont configurées pour le réseau de gestion. À partir de Gestionnaire de périphériques de pare-feu, configurez l'adresse et la passerelle dans **Device (Périphérique)** > **System Settings (Paramètres du système)** > **Management Interface (Interface de gestion)**. (Dans l'interface de ligne de commande, utilisez la commande **configure network ipv4/ipv6 manual**.)

  Remarque
  Assurez-vous d'utiliser une passerelle externe pour l'adresse IP de gestion. Vous ne pouvez pas utiliser les interfaces de données comme passerelle lors de l'utilisation d'un gestionnaire distant.

Étape 2 Pour passer de la gestion locale à la gestion à distance :

a) Vérifiez que vous êtes actuellement en mode de gestion locale.

```
> show managers
Managed locally.
```

b) Configurez le gestionnaire à distance.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*]

Lieu :

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} spécifie le nom d'hôte DNS ou l'adresse IP (IPv4 ou IPv6) du Centre de gestion Firepower (FMC) qui gère ce périphérique. Si Centre de gestion Firepower (FMC) n'est pas directement adressable, utilisez **DONTRESOLVE**. Si vous utilisez **DONTRESOLVE**, un *nat_id* est requis.
- *regkey* est la clé d'enregistrement alphanumérique unique nécessaire pour enregistrer un périphérique dans le Centre de gestion Firepower (FMC).
- *nat_id* est une chaîne alphanumérique facultative utilisée lors du processus d'enregistrement entre le Centre de gestion Firepower (FMC) et le périphérique. Elle est requise si le nom d'hôte (hostname) est défini sur DONTRESOLVE.

Par exemple, pour utiliser le gestionnaire à l'adresse 192.168.0.123 avec la clé d'enregistrement **secret**, saisissez ce qui suit :

```
> configure manager add 192.168.0.123 secret
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before switching to remote management.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue  [yes/no] yes
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.
```

```
> show managers
Host                    : 192.168.0.123
Registration Key        : ****
Registration            : pending
RPC Status              :
```

Remarque
Lorsque l'enregistrement est toujours en attente, vous pouvez utiliser **configure manager delete** pour annuler l'enregistrement, puis **configure manager local** pour revenir à la gestion locale.

c) Connectez-vous à Centre de gestion Firepower (FMC) et ajoutez le périphérique.

Consultez l'aide en ligne de Centre de gestion Firepower (FMC) pour connaître les étapes détaillées.

Étape 3 Pour passer de la gestion à distance à la gestion locale :

a) Vérifiez que vous êtes actuellement en mode de gestion à distance.

```
> show managers
Host                    : 192.168.0.123
Registration Key        : ****
Registration            : pending
RPC Status              :
```

b) Supprimez le gestionnaire distant et passez en mode sans gestionnaire.

Vous ne pouvez pas passer directement de la gestion à distance à la gestion locale. Utilisez la commande **configure manager delete** pour supprimer le gestionnaire.

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

c) Configurez le gestionnaire local.

configure manager local

Par exemple :

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

Vous pouvez maintenant utiliser un navigateur Web pour ouvrir le gestionnaire local à l'adresse **https://***management-IP-address*.

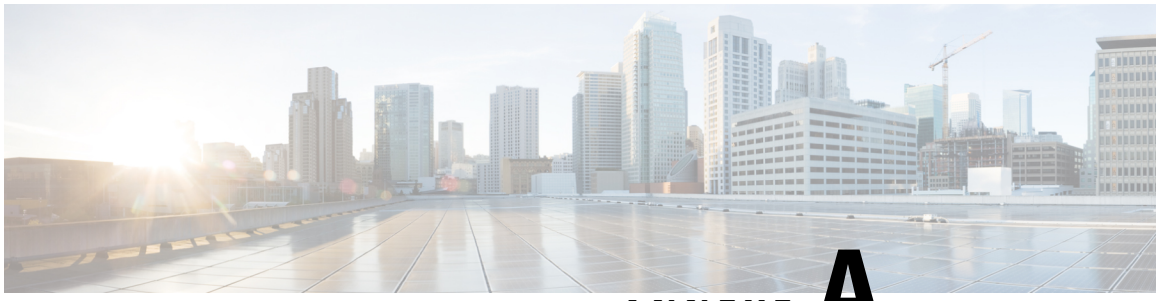
Tâches de gestion du matériel

Les rubriques suivantes expliquent comment effectuer certaines tâches de maintenance du matériel. Consultez les différents guides matériels pour obtenir des renseignements plus complets et des renseignements sur d'autres tâches de gestion du matériel.

Remplacement d'un périphérique ISA 3000

L'ISA 3000 dispose d'une carte SD que vous pouvez retirer et insérer dans un autre périphérique ISA 3000. Si vous créez des sauvegardes de système sur la carte SD, vous pouvez utiliser cette fonction pour remplacer facilement un périphérique. Il suffit de retirer la carte SD du périphérique défaillant et de l'insérer dans le nouveau périphérique. Les sauvegardes sont alors disponibles pour restauration.

Pour vous assurer d'avoir les sauvegardes nécessaires, configurez la tâche de sauvegarde pour créer la sauvegarde sur la carte SD.



ANNEXE A

Configuration avancée

Certaines fonctionnalités du périphérique sont configurées au moyen de commandes de configuration ASA. Bien que le Gestionnaire de périphériques de pare-feu puisse configurer de nombreuses fonctionnalités basées sur les commandes, il ne les prend pas en charge toutes. Si vous devez utiliser certaines de ces fonctionnalités ASA qui ne sont pas prises en charge dans Gestionnaire de périphériques de pare-feu, vous pouvez utiliser l'interface de ligne de commande Smart ou FlexConfig pour configurer manuellement les fonctionnalités.

Les rubriques suivantes expliquent ce type de configuration avancée plus en détail.

- À propos de Smart CLI et de FlexConfig , à la page 869
- Lignes directrices et limites de Smart CLI et FlexConfig, à la page 879
- Configuration des objets Smart CLI, à la page 880
- Configurer la politique FlexConfig, à la page 881
- Dépannage de la politique FlexConfig, à la page 893
- Exemples de FlexConfig, à la page 894

À propos de Smart CLI et de FlexConfig

FTD utilise des commandes de configuration ASA pour implémenter certaines fonctionnalités, mais pas toutes. Il n'y a pas d'ensemble unique de commandes de configuration Firepower Threat Defense.

Vous pouvez configurer les fonctionnalités de l'interface de ligne de commande en utilisant les méthodes suivantes :

- **Smart CLI** : (méthode préférée) Un modèle Smart CLI est un modèle prédéfini pour une fonctionnalité particulière. Toutes les commandes nécessaires à la fonctionnalité sont fournies, et vous devez simplement sélectionner les valeurs des variables. Le système valide votre sélection, ce qui vous permet de configurer plus facilement une fonctionnalité correctement. S'il existe un modèle Smart CLI pour la fonctionnalité souhaitée, vous devez utiliser cette méthode.
- **FlexConfig** : la politique FlexConfig est un ensemble d'objets FlexConfig. Les objets FlexConfig sont de forme plus libre que les modèles Smart CLI et le système n'effectue aucune validation de CLI, de variable ou de données. Vous devez connaître les commandes de configuration ASA et suivre les guides de configuration ASA pour créer une séquence valide de commandes.

L'objectif de Smart CLI et de FlexConfig est de vous permettre de configurer des fonctionnalités qui ne sont pas directement prises en charge par les politiques et les paramètres Gestionnaire de périphériques de pare-feu.

Mise en garde Cisco recommande fortement d'utiliser les Smart CLI et FlexConfig uniquement si vous êtes un utilisateur avancé avec de solides connaissances en ASA, et ce, à vos propres risques. Vous pouvez configurer des commandes qui ne sont pas interdites. L'activation de fonctionnalités par le biais de Smart CLI et FlexConfig peut entraîner des résultats imprévus avec d'autres fonctionnalités configurées.

Vous pouvez communiquer avec le Centre d'assistance technique de Cisco pour obtenir de l'aide concernant les objets Smart CLI et FlexConfig que vous avez configurés. Le Centre d'assistance technique de Cisco ne conçoit ni n'écrit de configurations personnalisées au nom d'un client. Cisco n'exprime aucune garantie quant au bon fonctionnement ni à l'interopérabilité avec d'autres Firepower Threat Defense fonctionnalités. Les fonctionnalités Smart CLI et FlexConfig peuvent être obsolètes à tout moment. Pour obtenir une prise en charge des fonctionnalités entièrement garantie, vous devez attendre le soutien Gestionnaire de périphériques de pare-feu. En cas de doute, n'utilisez pas Smart CLI ou FlexConfig.

Les rubriques suivantes expliquent ces fonctionnalités plus en détail.

Utilisation conseillée pour Smart CLI et FlexConfig

Il y a deux utilisations principales recommandées pour FlexConfig :

- Vous passez d'ASA à Firepower Threat Defense, et vous utilisez (et devez continuer à utiliser) des fonctions compatibles qui ne sont pas directement prises en charge par Gestionnaire de périphériques de pare-feu. Dans ce cas, utilisez la commande **show running-config** sur l'ASA pour afficher la configuration de la fonctionnalité et créez vos objets FlexConfig pour la mettre en œuvre. Vérifiez en comparant la sortie **show running-config** sur les deux périphériques.
- Vous utilisez Firepower Threat Defense, mais il y a un paramètre ou une fonctionnalité que vous devez configurer. Par exemple, le centre d'assistance technique de Cisco vous indique qu'un paramètre particulier devrait résoudre un problème précis que vous rencontrez. Pour les fonctionnalités complexes, utilisez un appareil de laboratoire pour tester FlexConfig et vérifiez que vous obtenez le comportement attendu.

Avant d'essayer de recréer une configuration ASA, déterminez d'abord si vous pouvez configurer une fonctionnalité équivalente dans les politiques standard. Par exemple, la politique de contrôle d'accès comprend la détection et la prévention des intrusions, HTTP et d'autres types d'inspection de protocole, le filtrage d'URL, le filtrage d'applications et le contrôle d'accès, que l'ASA met en œuvre à l'aide de fonctionnalités distinctes. Étant donné que de nombreuses fonctionnalités ne sont pas configurées à l'aide des commandes CLI, vous ne verrez pas toutes les politiques représentés dans la sortie de **show running-config**.

Remarque Gardez à tout moment à l'esprit qu'il n'y a pas de recouvrement direct entre ASA et Firepower Threat Defense. N'essayez pas de recréer complètement une configuration ASA sur un périphérique Firepower Threat Defense. Vous devez tester attentivement toute fonctionnalité que vous configurez à l'aide de FlexConfig.

Commandes CLI dans les objets Smart CLI et les objets FlexConfig

Le Firepower Threat Defense utilise des commandes de configuration ASA pour configurer certaines fonctionnalités. Bien que toutes les fonctionnalités de l'ASA ne soient pas compatibles avec le Firepower Threat Defense, certaines fonctionnalités peuvent fonctionner sur le Firepower Threat DefenseGestionnaire de périphériques de pare-feu, mais que vous ne pouvez pas configurer dans les politiques. Vous pouvez utiliser

Smart CLI et les objets FlexConfig pour préciser les commandes CLI requises pour configurer ces fonctionnalités.

Si vous décidez d'utiliser Smart CLI ou FlexConfig pour configurer manuellement une fonctionnalité, vous êtes responsable de connaître et de mettre en œuvre les commandes selon la syntaxe appropriée. FlexConfig ne valide pas la syntaxe des commandes CLI. Pour plus d'informations sur la syntaxe appropriée et la configuration des commandes CLI, utilisez la documentation d'ASA comme référence :

- Les guides de configuration de l'interface de ligne de commande ASA expliquent comment configurer une fonctionnalité. Vous trouverez les guides à l'adresse http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html
- Les références de commande ASA fournissent des informations supplémentaires triées par nom de commande. Vous trouverez les références à l'adresse http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html

Les rubriques suivantes expliquent plus en détail les commandes de configuration.

Incidence des mises à niveau logicielles sur la politique FlexConfig

Chaque nouvelle version du logiciel Firepower Threat Defense ajoute une prise en charge pour la configuration des fonctionnalités dans FDM. Parfois, ces nouvelles fonctionnalités peuvent chevaucher des fonctionnalités que vous avez précédemment configurées à l'aide de FlexConfig.

Après la mise à niveau, vous devez examiner la politique et les objets FlexConfig. Si l'un d'eux contient des commandes qui sont devenues interdites en raison de l'ajout d'une prise en charge dans FDM ou de l'interface de ligne de commande Smart, les icônes dans la liste des objets et les messages indiquent le problème. Veuillez prendre le temps de refaire votre configuration. Utilisez la liste des commandes interdites pour déterminer où les commandes doivent maintenant être configurées.

Le système ne vous empêchera pas de déployer des modifications lorsque les objets FlexConfig associés à la politique FlexConfig contiennent des commandes nouvellement interdites. Cependant, vous ne pourrez pas créer de nouveaux objets Smart CLI tant que vous n'aurez pas résolu tous les problèmes observés dans la politique FlexConfig.

Vous pouvez simplement supprimer les objets problématiques de la politique FlexConfig, car la restriction s'applique uniquement aux objets que vous déployez activement dans la configuration du périphérique. Ainsi, vous pouvez supprimer les objets, puis les utiliser comme référence lorsque vous créez l'interface de ligne de commande Smart correspondante ou avez intégré la configuration FDM. Une fois que vous êtes satisfait de la nouvelle configuration, vous pouvez simplement supprimer les objets. Si les objets supprimés contiennent des éléments non interdits, vous pouvez les modifier pour supprimer les commandes non prises en charge, puis rassocier les objets à la politique FlexConfig.

Déterminer la version du logiciel du périphérique ASA et la configuration actuelle de la CLI

Comme le système utilise les commandes du logiciel ASA pour configurer certaines fonctionnalités, vous devez déterminer la version actuelle de l'ASA utilisée dans le logiciel s'exécutant sur le périphérique Firepower Threat Defense. Ce numéro de version indique quels guides de configuration de CLI ASA utiliser pour obtenir des instructions sur la configuration d'une fonctionnalité. Vous devez également examiner la configuration actuelle basée sur l'interface de ligne de commande et la comparer à la configuration ASA que vous souhaitez mettre en œuvre.

Gardez à l'esprit que toute configuration ASA sera très différente d'une configuration Firepower Threat Defense. De nombreuses politiques Firepower Threat Defense sont configurées en dehors de la CLI, de sorte

que vous ne pouvez pas voir la configuration en regardant les commandes. N'essayez pas de créer de correspondance un à un entre une configuration ASA et Firepower Threat Defense.

Pour afficher ces informations, soit ouvrez la console CLI dans le Gestionnaire de périphériques de pare-feu, soit établissez une connexion SSH à l'interface de gestion du périphérique et saisissez les commandes suivantes :

- **show version system** et recherchez le numéro de la version logicielle du périphérique de sécurité adaptatif Cisco.
- **show running-config** pour afficher la configuration actuelle de l'interface de ligne de commande.
- **show running-config all** pour inclure toutes les commandes par défaut dans la configuration actuelle de l'interface de ligne de commande.

Commandes CLI interdites

Le but de Smart CLI et FlexConfig est de configurer les fonctionnalités disponibles sur les périphériques ASA que vous ne pouvez pas configurer sur les périphériques Firepower Threat Defense à l'aide du Gestionnaire de périphériques de pare-feu.

Ainsi, vous ne pouvez pas configurer les fonctionnalités ASA qui ont des équivalents dans Gestionnaire de périphériques de pare-feu. Le tableau suivant répertorie certaines de ces zones de commande interdites. Cette liste contient de nombreuses commandes parentes qui passent en mode de configuration. L'interdiction de la commande parente entraîne également l'interdiction des commandes enfants. Elle comprend également la version **no** des commandes et les commandes **clear** associées.

L'éditeur d'objet FlexConfig vous empêche d'inclure ces commandes dans l'objet. Cette liste ne s'applique pas aux modèles Smart CLI, car ils comprennent uniquement les commandes que vous pouvez configurer validement.

Commandes CLI interdites	Commentaires
aaa	Utilisez **Objects (Objets)** > **Identity Sources (Sources d'identité)**.
aaa-server	Utilisez **Objects (Objets)** > **Identity Sources (Sources d'identité)**.
access-list	Partiellement bloqué. • Vous pouvez créer des listes d'accès **ethertype**. • Vous ne pouvez pas créer de listes d'accès **extended** et **standard**. Créez ces ACL à l'aide des objets Liste d'accès étendue ou Liste d'accès standard de Smart CLI. Vous pouvez ensuite les utiliser sur les commandes prises en charge par FlexConfig qui font référence à la liste de contrôle d'accès par nom d'objet, comme **match access-list** avec une liste de contrôle d'accès étendue pour les classes de trafic des politiques de service. • Vous ne pouvez pas créer de listes d'accès **advanced**, que le système utilise avec la commande **access-group**. Au lieu de cela, utilisez **Policies (Politiques)** > **Access Control (Contrôle d'accès)** pour configurer les critères d'accès. • Vous ne pouvez pas créer de listes d'accès **webtype**.

Commandes CLI interdites	Commentaires
anyconnect-custom-data	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** pour configurer client AnyConnect.
asdm	Cette fonctionnalité ne s'applique pas à un système Firepower Threat Defense.
as-path	Créez des objets de chemin AS pour Smart CLI et utilisez-les dans un objet BGP Smart CLI pour configurer un filtre de chemin de système autonome.
attribute	—
auth-prompt	Cette fonctionnalité ne s'applique pas à un système Firepower Threat Defense.
boot	—
call-home	—
captive-portal	Utilisez **Policies (Politiques)** > **Identity (Identité** pour configurer le portail captif utilisé pour l'authentification active.
clear	—
client-update	—
clock	Utilisez **Device (Périphérique)** > **System Settings (Paramètres du système)** > **NTP** pour configurer l'heure du système.
cluster	—
command-alias	—
community-list	Créez des objets de liste de communauté étendue ou de liste de communauté standard Smart CLI et utilisez-les dans un objet BGP Smart CLI pour configurer un filtre de liste de communauté.
compression	—
configure	—
crypto	Sur la page **Objects** (Objets), utilisez **Certificates** (Certificats), **IKE Policies** (Politiques IKE), et **IPSec Proposals** (Propositions IPSec).
dhcp-client	—
dhcpd	Utilisez **Device (Périphérique)** > **System Settings (Paramètres du système)** > **DHCP Server (Serveur DHCP)**. Cependant, la commande **dhcpd option** est autorisée.
dhcprelay	Utilisez plutôt la ressource dhcprelayservices dans l'API .

Commandes CLI interdites	Commentaires
dns	**Objects (Objets)** > **DNS Groups (Groupes DNS)** : vous pouvez maintenant configurer des groupes DNS à l'aide de **Device (Périphérique)** > **System Settings (Paramètres système)** > **DNS Server (Serveur DNS)**.
dns-group	**Objects (Objets)** > **DNS Groups (Groupes DNS)** : vous pouvez maintenant configurer des groupes DNS à l'aide de **Device (Périphérique)** > **System Settings (Paramètres système)** > **DNS Server (Serveur DNS)**.
domain-name	**Objects (Objets)** > **DNS Groups (Groupes DNS)** : vous pouvez maintenant configurer des groupes DNS à l'aide de **Device (Périphérique)** > **System Settings (Paramètres système)** > **DNS Server (Serveur DNS)**.
dynamic-access-policy-config **dynamic-access-policy-record**	—
enable	—
event	—
failover	—
fips	—
firewall	Gestionnaire de périphériques de pare-feu ne prend en charge que le mode de pare-feu routé.
hostname	Utilisez **Device (Périphérique)** > **System Settings (Paramètres système)** > **Hostname (Nom d'hôte)**.
hpm	Cette fonctionnalité ne s'applique pas à un système Firepower Threat Defense.
http	Utilisez l'onglet **Data Interfaces** (Interfaces de données) sur **Device (Périphérique)** > **System Settings (Paramètres système)** > **Management Access (Accès à l'interface de gestion**.
inline-set	—

Commandes CLI interdites	Commentaires
interface pour les BVI, l'interface de gestion, Ethernet, GigabitEthernet et les sous-interfaces.	Partiellement bloqué. Configurez les interfaces physiques, les sous-interfaces et les interfaces virtuelles de pont sur la page **Device (Périphérique)** > **Interfaces**. Vous pouvez ensuite configurer des options supplémentaires à l'aide de FlexConfig. Cependant, les commandes en mode **interface** suivantes sont interdites pour ces types d'interface. **cts** **ip address** **ip address dhcp** **ipv6 address** **ipv6 enable** **ipv6 nd dad** **ipv6 nd suppress-ra** **mode** **nameif** **security-level** **shutdown** **zone-member**
interface pour **vni**, **redundant**, **tunnel**	Configurez les interfaces sur la page **Device (Périphérique)** > **Interfaces**. Gestionnaire de périphériques de pare-feu ne prend pas en charge ces types d'interface.
ip audit	Cette fonctionnalité ne s'applique pas à un système Firepower Threat Defense. Appliquez plutôt les politiques d'intrusion à l'aide des règles de contrôle d'accès.
ip-client	Pour configurer le système afin qu'il utilise les interfaces de données comme passerelle de gestion, utilisez **Device (Périphérique)** > **ystem Settings (Paramètres système)** > **Management Interface (Interface de gestion)**.
ip local pool	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** pour configurer des ensembles d'adresses.
ipsec	—
ipv6	Créez des objets de liste de préfixes IPv6 Smart CLI et utilisez-les dans un objet Smart CLI BGP pour configurer le filtrage de liste de préfixes pour IPv6.
ipv6-vpn-addr-assign	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** pour configurer des ensembles d'adresses.
isakmp	Utilisez **Device (Périphérique)** > **Site-to-Site VPN (VPN de site à site)**.

Commandes CLI interdites	Commentaires
jumbo-frame	Le système active automatiquement la prise en charge des trames étendues si vous augmentez la MTU de n'importe quelle interface au-delà de la valeur par défaut de 1 500.
ldap	—
license-server	Utilisez **Device (Périphérique)** > **Smart License (Licence Smart)**.
logging	Utilisez **Objects (Objets)** > **Syslog Servers (Serveurs Syslog)** et **Device (Périphérique)** > **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation)**. Cependant, vous pouvez configurer la commande **logging history** dans FlexConfig.
management-access	—
migrate	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** et **Device (Périphérique)** > **Site-to-Site VPN (VPN de site à site)** pour activer la prise en charge d'IKEv2.
mode	Gestionnaire de périphériques de pare-feu ne prend en charge que le mode à contexte unique.
mount	—
mtu	Configurez la MTU par interface sur **Device (Périphérique)** > **Interfaces**.
nat	Utilisez **Policies (Politiques)** > **NAT**.
ngips	—
ntp	Utilisez **Device (Périphérique)** > **System Settings (Paramètres système)** > **NTP**
object-group network **object network**	Utilisez **Objects (Objets)** > **Network (Réseau)**. Vous ne pouvez pas créer d'objets réseau ou de groupes dans FlexConfig, mais vous pouvez utiliser, en tant que variables, les objets réseau et groupes définis dans le gestionnaire d'objets à l'intérieur du modèle.
object service |natorigsvc **object service |natmappedsvc**	La commande **object service** st généralement autorisée, mais vous ne pouvez pas modifier les objets internes nommés |natorigsvc ou |natmappedsvc. Dans ces noms, la barre verticale est intentionnelle et il s'agit du premier caractère des noms d'objets restreints.
passwd **password**	—
password-policy	—

Commandes CLI interdites	Commentaires
policy-list	Créez des objets de liste des politiques Smart CLI et utilisez-les dans un objet Smart CLI BGP pour configurer une liste des politiques.
policy-map sous-commandes	Vous ne pouvez pas configurer les commandes suivantes dans une liste des politiques. **priority** **police** **match tunnel-group**
prefix-list	Créer des objets de liste de préfixes IPv4 Smart CLI et les utiliser dans un objet Smart CLI OSPF ou BGP pour configurer le filtrage des listes de préfixes IPv4.
priority-queue	—
privilege	—
reload	Vous ne pouvez pas planifier de rechargements. Le système n'utilise pas la commande **reload** pour redémarrer le système, il utilise la commande **reboot**.
rest-api	Cette fonctionnalité ne s'applique pas à un système Firepower Threat Defense. L'API REST est toujours installée et activée.
route	Utilisez **Device (Périphérique)** > **Routing (Routage)** pour configurer les routes statiques.
route-map	Créer des objets de carte de routage Smart CLI et les utiliser dans un objet Smart CLI OSPF ou BGP pour configurer des cartes de routage.
router bgp	Utilisez les modèles Smart CLI pour BGP.
router eigrp	Utilisez les modèles Smart CLI pour EIGRP.
router ospf	Utilisez les modèles Smart CLI pour OSPF.
scansafe	Cette fonctionnalité ne s'applique pas à un système Firepower Threat Defense. Configurez plutôt le filtrage d'URL dans les règles de contrôle d'accès.
setup	Cette fonctionnalité ne s'applique pas à un système Firepower Threat Defense.
sla	—
snmp-server	Utilisez les ressources SNMP de l'API FTP pour configurer SNMP.
ssh	Utilisez l'onglet **Data Interfaces** (Interfaces de données) sur **Device (Périphérique)** > **System Settings (Paramètres système)** > **Management Access (Accès à l'interface de gestion**.

Commandes CLI interdites	Commentaires
ssl	Utilisez **Device (Périphérique)** > **System Settings (Paramètres système)** > **SSL Settings (Paramètres SSL)**
telnet	Firewall Threat Defense ne prend pas en charge les connexions Telnet. Utilisez SSH au lieu de Telnet pour accéder à l'interface de ligne de commande du périphérique.
time-range	—
tunnel-group	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** et **Device (Périphérique)** > **Site-to-Site VPN (VPN de site à site)**.
tunnel-group-map	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** et **Device (Périphérique)** > **Site-to-Site VPN (VPN de site à site)**.
user-identity	Utiliser **Policies (Politiques)** > **Identity (Identité)**.
username	Pour créer des utilisateurs d'interface de ligne de commande, ouvrez une session SSH ou de console sur le périphérique et utilisez les commandes **configure user**.
vpdn	—
vpn	—
vpn-addr-assign	—
vpnclient	—
vpn-sessiondb	—
vpnsetup	—
webvpn	—
zone	—
zonelabs-integrity	Cette fonctionnalité ne s'applique pas à un système Firepower Threat Defense.

Modèles Smart CLI

Le tableau suivant explique les modèles d'interface de ligne de commande Smart en fonction de la fonctionnalité.

Remarque Vous configurez également OSPF et BGP à l'aide des modèles Smart CLI. Cependant, ces modèles sont disponibles dans la page **Device (Périphérique)** > **Routing (Routage)** plutôt que dans la page de configuration avancée.

Fonctionnalités	Modèles	Description
Objets : AS Path	ASPath	Créez des objets ASPath à utiliser avec des objets de protocole de routage.
Objets : Access List (liste d'accès)	Liste d'accès étendue Liste d'accès standard	Créez des listes de contrôle d'accès étendues ou standard à utiliser avec des objets de routage. Vous pouvez également faire référence à ces objets par nom à partir des objets FlexConfig qui configurent les commandes autorisées qui utilisent les listes de contrôle d'accès.
Objets : Community List (liste de communautés)	Liste de communauté élargie Liste de communauté standard	Créez des listes de communauté étendues ou standard à utiliser avec des objets de routage.
Objets : Prefix List (liste de préfixes)	Liste des préfixes IPV4 Liste des préfixes IPV6	Créez des listes de préfixes IPv4 ou IPv6 à utiliser avec des objets de routage.
Objets : Policy List (liste de politiques)	Liste des stratégies	Créez des listes de politiques à utiliser avec des objets de routage.
Objets : Route Map (Carte de routage)	Carte de routage	Créez des cartes de routage à utiliser avec des objets de routage.

Lignes directrices et limites de Smart CLI et FlexConfig

Veuillez garder les éléments suivants à l'esprit lors de la configuration des fonctionnalités par le biais de l'interface de ligne de commande Smart ou de FlexConfig.

- Les commandes définies dans les objets FlexConfig sont déployées après toutes les commandes pour les fonctionnalités définies par Gestionnaire de périphériques de pare-feu, y compris Smart CLI. Ainsi, vous pouvez dépendre des objets, des interfaces, etc. configurés avant que ces commandes ne soient transmises au périphérique. Si vous devez utiliser un élément déployé par FlexConfig dans un modèle d'interface de ligne de commande Smart, créez et déployez FlexConfig avant de créer et de déployer le modèle d'interface de ligne de commande Smart. Par exemple, si vous souhaitez utiliser le modèle d'interface de ligne de commande Smart OSPF pour redistribuer les routes EIGRP, utilisez d'abord FlexConfig pour configurer EIGRP, puis créez le modèle d'interface de ligne de commande Smart OSPF.
- Si vous souhaitez supprimer une fonctionnalité ou une partie d'une fonctionnalité que vous avez configurée par le biais de FlexConfig, mais qu'un modèle d'interface de ligne de commande Smart fait référence à

cette fonctionnalité, vous devez d'abord supprimer les commandes du modèle d'interface de ligne de commande Smart qui utilisent la fonctionnalité. Ensuite, déployez la configuration afin que la fonctionnalité configurée via Smart CLI n'y fasse plus référence. Vous pouvez ensuite supprimer la fonctionnalité de FlexConfig, puis redéployer la configuration afin de l'éliminer complètement.

Configuration des objets Smart CLI

Les objets Smart CLI définissent des fonctionnalités qui ne peuvent pas être configurées ailleurs dans le Gestionnaire de périphériques de pare-feu. Les objets Smart CLI fournissent un niveau d'accompagnement pour configurer une fonctionnalité. Pour une fonctionnalité (modèle) donnée, toutes les commandes possibles sont préchargées et les variables que vous saisissez sont validées. Ainsi, bien que vous utilisiez toujours les commandes CLI pour configurer une fonctionnalité, les objets Smart CLI ne sont pas aussi libres que les objets FlexConfig.

Bien que les modèles Smart CLI fournissent un certain encadrement, vous devez toujours lire les guides de configuration ASA et les références de commande pour comprendre l'utilisation des commandes afin de choisir des valeurs qui fonctionnent correctement pour votre réseau. Idéalement, vous avez déjà une configuration ASA à partir de laquelle travailler et vous n'avez qu'à créer la même séquence de commandes dans l'objet Smart CLI.

Les objets Smart CLI sont regroupés selon le domaine de fonctionnalité.

Remarque Tous les objets Smart CLI que vous définissez sont déployés. Contrairement à FlexConfig, vous ne pouvez pas créer plusieurs objets Smart CLI, puis sélectionner lequel déployer. Créez des objets Smart CLI uniquement pour les fonctionnalités que vous souhaitez configurer.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur la zone de fonctionnalité appropriée sous **Smart CLI** dans la table des matières de Advanced Configuration (Configuration avancée).

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Entrez un nom pour l'objet et, facultativement, une description.

Étape 5 Sélectionnez le **CLI Template** (Modèle CLI) pour la fonctionnalité que vous configurez.

Le système charge le modèle de commande dans la fenêtre **Template** (Modèle). Au départ, seules les commandes requises sont affichées. Il s'agit de la configuration minimale requise pour le modèle.

Étape 6 Remplissez les variables et ajoutez des commandes selon les besoins dans le modèle.

Idéalement, vous utilisez une configuration existante provenant d'un appareil ASA ou Firewall Threat Defense (géré par FMC). Avec une configuration en main, vous devez simplement rendre le modèle conforme à celle-ci, en modifiant des variables telles que les adresses IP et les noms d'interfaces en fonction de l'emplacement de cet appareil spécifique dans votre réseau.

Voici quelques conseils pour remplir le modèle :

- Pour sélectionner une valeur pour une variable, cliquez sur la variable et saisissez la valeur appropriée ou sélectionnez-la dans une liste (dans le cas des valeurs énumérées). Le déplacement du curseur sur les variables qui nécessitent une saisie affiche les valeurs valides pour l'option, comme une plage de nombres. Dans certains cas, la valeur conseillée est mentionnée.

  Par exemple, dans le modèle OSPF, la commande requise **router ospf** *process-id* affiche « Process ID (ID de processus) (1-65535) » au survol de la souris, et lorsque vous cliquez sur *process-id*, le champ est mis en surbrillance. Tapez simplement le numéro que vous souhaitez.

- Lorsque vous sélectionnez une option pour une variable, s'il existe d'autres commandes possibles pour configurer l'option, celles-ci sont automatiquement affichées et désactivées ou activées, le cas échéant. Surveillez ces commandes supplémentaires.

- Utilisez le lien **Show**/**Hide Disabled** (Afficher/Masquer désactivés) au-dessus du modèle pour contrôler l'affichage. Les commandes désactivées ne seront pas configurées, mais vous devez les afficher pour les configurer. Pour voir le modèle complet, cliquez sur le lien **Show Disabled** (Afficher désactivés) au-dessus du modèle. Pour voir uniquement les commandes qui seront configurées, cliquez sur le lien **Hide Disabled (Masquer désactivés)** au-dessus du tableau.

- Pour effacer toutes vos modifications depuis le dernier enregistrement de l'objet, cliquez sur le lien **Reset** (Réinitialiser) au-dessus du modèle.

- Pour activer une commande facultative, cliquez sur le bouton **+** à gauche du numéro de ligne.

- Pour désactiver une commande facultative, cliquez sur le bouton **-** à gauche du numéro de ligne. Si vous avez modifié la ligne, vos modifications ne sont pas supprimées.

- Pour dupliquer une commande, cliquez sur le bouton Options **...** et sélectionnez **Duplicate** (Dupliquer). Vous êtes autorisé à dupliquer les commandes uniquement s'il est valide d'entrer la commande plus d'une fois.

- Pour supprimer une commande en double, cliquez sur le bouton Options **...** et sélectionnez **Delete (Supprimer)**. Vous ne pouvez pas supprimer les commandes qui font partie du modèle de base.

Étape 7 Cliquez sur **OK**.

Configurer la politique FlexConfig

La politique FlexConfig est simplement une liste des objets FlexConfig que vous souhaitez déployer dans la configuration du périphérique. Seuls les objets inclus dans la politique sont déployés, tous les autres sont simplement définis et inutilisés.

Les commandes définies dans les objets FlexConfig sont déployées après toutes les commandes pour les fonctionnalités définies par Gestionnaire de périphériques de pare-feu, y compris Smart CLI. Ainsi, vous

pouvez dépendre des objets, des interfaces, etc. configurés avant que ces commandes ne soient transmises au périphérique. Si vous devez utiliser un élément déployé par FlexConfig dans un modèle d'interface de ligne de commande Smart, créez et déployez FlexConfig avant de créer et de déployer le modèle d'interface de ligne de commande Smart. Par exemple, si vous souhaitez utiliser le modèle d'interface de ligne de commande Smart OSPF pour redistribuer les routes EIGRP, utilisez d'abord FlexConfig pour configurer EIGRP, puis créez le modèle d'interface de ligne de commande Smart OSPF.



Remarque S'il existe un modèle d'interface de ligne de commande Smart pour une fonctionnalité, vous ne pouvez pas la configurer à l'aide de FlexConfig. Vous devez utiliser l'objet Smart CLI.

Avant de commencer

Créer les objets FlexConfig. Consultez les rubriques suivantes:

- Configurer les objets FlexConfig, à la page 883
- Création de variables dans un objet FlexConfig, à la page 885
- Configuration des objets de clé secrète, à la page 892

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Policy (Politique FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Gérer la liste des objets dans la **Group List** (Liste des groupes).

- Pour créer un objet, cliquez sur le bouton **+**. Si l'objet n'existe pas encore, cliquez sur **Create New FlexConfig Object** (Créer un nouvel objet FlexConfig) pour le définir.
- Pour supprimer un objet, cliquez sur le bouton **X** à droite de l'entrée de l'objet.

Remarque
Nous recommandons que chaque objet soit complètement autonome et ne dépende pas de la configuration définie dans un autre objet FlexConfig. Cela vous permet d'ajouter ou de supprimer des objets sans affecter les autres objets.

Étape 4 Évaluez les commandes proposées dans le volet **Preview** (Aperçu).

Vous pouvez cliquer sur le bouton **Expand** (Développer) (puis **Collapse** (Réduire)) pour élargir l'écran afin de pouvoir voir les commandes longues plus clairement.

L'aperçu évalue les variables et produit les commandes exactes qui seront émises. Assurez-vous que ces commandes sont correctes et valides. Vous êtes responsable de vous assurer que les commandes n'entraîneront pas d'erreurs ou de mauvaises configurations qui rendront l'appareil inutilisable.

Mise en garde
Le système ne valide pas les commandes. Il vous est possible de déployer des commandes non valides et même potentiellement destructrices. Examinez l'aperçu très attentivement avant de déployer les modifications.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

Après avoir modifié la politique FlexConfig, examinez attentivement les résultats du prochain déploiement. S'il y a des erreurs, corrigez l'interface de ligne de commande dans l'objet. Consultez Dépannage de la politique FlexConfig, à la page 893.

Configurer les objets FlexConfig

Un objet FlexConfig contient les commandes ASA nécessaires pour configurer une fonctionnalité particulière que vous ne pouvez pas configurer autrement à l'aide de Gestionnaire de périphériques de pare-feu. Vous êtes responsable de vous assurer de saisir la bonne séquence de commandes, sans faute de frappe. Le système ne valide pas le contenu des objets FlexConfig.

Nous vous recommandons de créer des objets distincts pour chaque fonctionnalité générale que vous souhaitez configurer. Par exemple, si vous souhaitez définir des bannières et configurer le protocole de routage RIP, utilisez 2 objets distincts. L'isolation des fonctionnalités dans des objets distincts vous permet de sélectionner plus facilement les objets à déployer et facilite le dépannage.

Remarque N'incluez pas les commandes **enable** et **configure terminal**. Le système passe automatiquement en mode adéquat pour les commandes de configuration.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Entrez un nom pour l'objet et, facultativement, une description.

Étape 5 Dans la section **Variables**, créez les variables que vous souhaitez utiliser dans le corps de l'objet.

Les seules variables que vous devez créer sont celles qui pointent vers des objets définis dans le Gestionnaire de périphériques de pare-feu, en particulier les types de variables de réseau, de port et de clé secrète, ou la variable d'interface, qui pointe vers une interface nommée. Pour les autres types de variables, vous pouvez simplement saisir les valeurs dans le corps de l'objet.

Pour des informations détaillées sur la création et l'utilisation des variables, consultez Création de variables dans un objet FlexConfig, à la page 885.

Étape 6 Dans la section **Template** (Modèle), saisissez les commandes ASA requises pour configurer la fonctionnalité.

Vous devez entrer les commandes dans le bon ordre pour configurer la fonctionnalité. Utilisez les guides de configuration de l'interface de ligne de commande ASA pour apprendre comment saisir les commandes. Idéalement, vous devriez avoir un fichier de configuration prétesté provenant d'un ASA ou d'un autre périphérique Firepower Threat Defense que vous pouvez utiliser comme référence.

Vous pouvez également utiliser la notation Mustache pour faire référence et traiter les variables. Pour de plus amples renseignements, voir Référence aux variables FlexConfig et récupération de leurs valeurs, à la page 886.

Voici quelques conseils pour la création du corps de l'objet :

- Pour ajouter des lignes, placez le curseur à la fin d'une ligne et appuyez sur Entrée.
- Pour utiliser une variable, saisissez le nom de la variable entre doubles accolades : {{*variable_name*}}. Pour les variables qui font référence à des objets, vous devez inclure l'attribut dont vous récupérez la valeur : {{*variable_name.attribut*}}. Les attributs disponibles varient selon le type d'objet. Pour obtenir des renseignements complets, consultez Références de variable : {{variable}} ou {{{variable}}}, à la page 886.
- Pour utiliser un objet Smart CLI, saisissez le nom de l'objet. Si vous devez faire référence à un processus de routage configuré dans Smart CLI, saisissez l'identifiant du processus. Consultez Référence aux objets Smart CLI dans un objet FlexConfig, à la page 891.
- Cliquez sur le lien **Expand/Collapse** (Développer/Réduire) au-dessus du corps du modèle pour agrandir ou réduire ce dernier.
- Cliquez sur le lien **Reset** (Réinitialiser) pour effacer toutes les modifications que vous avez apportées depuis le dernier enregistrement de l'objet.

Étape 7 Dans la section **Negate Template** (Modèle de négation), saisissez les commandes nécessaires pour supprimer ou inverser les commandes configurées dans le corps de l'objet.

La section de négation est très importante et sert deux objectifs :

- Cela simplifie le déploiement. Avant de redéployer les commandes dans le corps, le système utilise ces commandes pour d'abord effacer ou annuler la configuration. Cela garantit un déploiement propre.
- Si vous décidez de supprimer la fonctionnalité en supprimant l'objet de la politique FlexConfig, le système utilise ces commandes pour supprimer les commandes du périphérique.

Si vous décidez de supprimer la fonctionnalité en retirant l'objet de la FlexConfig Policy (Politique FlexConfig), le système utilise ces commandes pour supprimer les commandes du périphérique. Cela prendra plus de temps pour le déploiement et perturbera le trafic. Assurez-vous que vous disposez de toutes et uniquement des commandes nécessaires pour annuler la configuration définie dans le corps de l'objet. Bien que les commandes d'annulation soient généralement sous la forme **no** ou **clear** des commandes du modèle, si vous désactivez une fonctionnalité qui était déjà activée, la commande « negate » (annuler) est en fait la forme positive de la commande, celle qui active la fonctionnalité.

Utilisez les guides de configuration ASA et la référence de commande pour déterminer les commandes appropriées. Parfois, vous pouvez annuler une configuration avec une seule commande. Par exemple, dans un objet qui configure RIP, une simple commande **no router rip** supprime l'ensemble de la configuration **router rip**, y compris les sous-commandes.

De même, si vous avez saisi plusieurs commandes **banner login** pour créer une bannière multilignes, une seule commande **no banner login** annule l'ensemble de la bannière de connexion.

Si votre modèle crée plusieurs objets imbriqués, le modèle d'annulation doit supprimer les objets dans l'ordre inverse, pour supprimer d'abord les références aux objets avant de supprimer les objets. Par exemple, si vous créez d'abord une liste de contrôle d'accès, puis y faites référence dans une classe de trafic, puis faites référence à la classe de trafic dans une carte de politiques et activez finalement la carte de politiques à l'aide d'une politique de service, le modèle d'annulation doit d'abord annuler la configuration en supprimant la politique de service, puis la carte de politiques, puis la classe de trafic et finalement l'ACL.

Étape 8 Cliquez sur **OK**.

Prochaine étape

La simple création d'un objet FlexConfig ne suffit pas pour le déployer. Vous devez ajouter l'objet à la politique FlexConfig. Seuls ces objets de la politique FlexConfig sont déployés. Cela vous permet d'affiner vos objets FlexConfig et d'en avoir certains prêts pour des utilisations spéciales, sans qu'ils soient tous automatiquement déployés. Consultez Configurer la politique FlexConfig, à la page 881.

Création de variables dans un objet FlexConfig

Les variables que vous utilisez dans un objet FlexConfig sont définies dans l'objet lui-même. Il n'y a pas de liste distincte de variables. Ainsi, vous ne pouvez pas définir une variable puis l'utiliser dans des objets FlexConfig distincts.

Les variables fournissent ces principaux avantages :

- Ils permettent de pointer vers des objets définis à l'aide de Gestionnaire de périphériques de pare-feu. Cela inclut les objets de réseau, de port et de clé secrète.
- Ils isolent les valeurs qui pourraient changer à partir du corps de l'objet. Ainsi, si vous devez modifier une valeur, vous modifiez simplement la variable et vous n'avez pas besoin de modifier le corps de l'objet. Cela peut être particulièrement utile si vous devez faire référence à l'objet dans plusieurs lignes de commande.

Cette procédure explique le processus d'ajout de variables à un objet FlexConfig.

Procédure

Étape 1 Modifier ou créer un objet FlexConfig à partir de la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Consultez Configurer les objets FlexConfig, à la page 883.

Étape 2 Effectuez l'une des opérations suivantes dans la section **Variables** :

- Pour ajouter une variable, cliquez sur le bouton **+** (ou cliquez sur **Add Variable** (Ajouter une variable) s'il n'y en a aucune encore définie).
- Pour modifier une variable, cliquez sur l'icône de modification ( ) en regard de la variable.

Pour supprimer une variable, cliquez sur l'icône de la corbeille ( ) pour cette variable. Assurez-vous de supprimer toutes les références à cette variable dans le corps du modèle.

Étape 3 Saisissez un nom pour la variable et, au besoin, une description.

Étape 4 Sélectionnez un **type** de données pour la variable, puis saisissez ou sélectionnez la valeur.

Vous pouvez créer les types de variables suivants. Choisissez un type qui correspond aux exigences de données des commandes dans lesquelles vous utiliserez la variable.

- **Chaîne** : une chaîne de texte. Par exemple, les noms d'hôte, les noms d'utilisateur, etc.
- **Numérique** : un nombre entier. N'incluez pas de virgules, de décimales, de signes (comme le signe négatif) ou la notation hexadécimale. Pour les nombres non entiers, utilisez une variable de chaîne.
- **Booléen** : une valeur logique vraie ou fausse. Sélectionnez Vrai ou Faux.
- **Objet réseau** : un objet réseau ou un groupe défini sur la page Objets. Sélectionnez l'objet réseau ou le groupe.
- **Objet de port** : un objet de port TCP ou UDP défini sur la page Objets. Sélectionnez l'objet de port. Vous ne pouvez pas sélectionner de groupes ou d'objets pour d'autres protocoles.
- **Interface** : une interface nommée définie sur la page Device (Périphérique) > Interfaces. Sélectionnez l'interface. Vous ne pouvez pas sélectionner d'interfaces qui n'ont pas de nom.
- **Adresse IP** : une adresse IP IPv4 ou IPv6 unique, sans masque réseau ni longueur de préfixe.
- **Clé secrète** : un objet de clé secrète défini pour FlexConfig. Sélectionnez l'objet. Pour en savoir plus sur la création d'objets de clé secrète, consultez Configuration des objets de clé secrète, à la page 892.

Étape 5 Cliquez sur **Add** (Ajouter) ou **Save** (Enregistrer) dans la boîte de dialogue Variable.

Vous pouvez maintenant utiliser la variable dans le corps de l'objet FlexConfig. La façon dont vous faites référence à la variable diffère en fonction du type de variable. Pour plus de détails sur l'utilisation de ces variables, consultez les rubriques suivantes :

- Références de variable : {{variable}} ou {{{variable}}}, à la page 886
- Sections {{#key}} {{/key}} et sections inverses {{^key}} {{/key}}, à la page 889

Étape 6 Cliquez sur **OK** dans la boîte de dialogue de l'objet FlexConfig.

Référence aux variables FlexConfig et récupération de leurs valeurs

FlexConfig utilise Mustache comme langue de modèle, mais la prise en charge est limitée aux fonctionnalités expliquées dans les sections suivantes. Utilisez ces fonctionnalités pour faire référence aux variables, récupérer leurs valeurs et les traiter.

Références de variable : {{variable}} ou {{{variable}}}

Pour faire référence à une variable, que vous définissez dans un objet FlexConfig, utilisez la notation suivante :

{{*variable_name*}}

Ou :

{{{*variable_name*}}}

Cela est suffisant pour les variables simples qui sont des valeurs uniques, qui comprennent les variables des types suivants : **Numeric** (Numérique), **String** (Chaîne), **Boolean** (Booléen) et **IP**. Utilisez des accolades triples si la variable contient des caractères spéciaux tels que &. Sinon, vous pouvez toujours utiliser des accolades triples pour toutes les variables.

Toutefois, pour les variables qui pointent vers des éléments modélisés comme des objets dans la base de données de configuration, vous devez utiliser la notation par points et inclure le nom de l'attribut de l'objet que vous souhaitez récupérer. Vous pouvez trouver ces noms d'attribut en examinant les modèles dans l'outil API Explorer (Explorateur d'API) pour le type d'objet associé. Vous devez utiliser la notation suivante pour utiliser les variables des types suivants : **Secret**, **Network** (Réseau), **Port** et **Interface**.

{{*variable_name.attribute*}}

Par exemple, pour récupérer l'adresse d'une variable réseau nommée net-object1 (qui pointe vers un objet réseau, et non un groupe réseau), vous utiliserez :

{{net-object1.value}}

Si vous essayez de récupérer une valeur d'attribut d'un objet dans un objet, vous devez utiliser une série d'attributs séparés par des points pour accéder à la valeur souhaitée. Par exemple, les adresses IP d'une interface sont modélisées comme des sous-objets, nommés ipv4 et ipv6, dans l'objet de l'interface. Ainsi, pour récupérer l'adresse IPv4 et le masque de sous-réseau d'une variable d'interface nommée int-inside (qui pointe vers l'interface interne), vous utiliserez :

{{int-inside.ipv4.ipAddress.ipAddress}} {{int-inside.ipv4.ipAddress.netmask}}

Remarque Pour ouvrir l'explorateur d'API, cliquez sur le bouton more options (plus d'options) (⋮) et choisissez **API Explorer** (Explorateur d'API).

Le tableau suivant répertorie les types de variables, la façon de les référencer et, pour les objets, le nom du modèle API et les références les plus susceptibles d'être utilisées.

Type de variable	Modèles de référence	Description
Booléen (variable simple)	**Variable :** {{*variable_name*}} **Section :** `{{#variable_name}}` `commands` `{{/variable_name}}` **Section inverse :** `{{^variable_name}}` `commands` `{{/variable_name}}`	Une valeur logique vrai/faux. L'objectif principal des variables booléennes est de contrôler des sections ou des sections inverses. Vous pouvez modifier la valeur d'une variable booléenne pour activer ou désactiver une section de commandes, par exemple, si vous devez activer une fonctionnalité périodiquement ou dans des circonstances spéciales uniquement. Certains objets ont également des attributs booléens dans leurs modèles, que vous pouvez utiliser pour fournir le traitement facultatif d'une section.

Type de variable	Modèles de référence	Description
Interface (variable d'objet : le modèle API est Interface)	**Variable :** {{*variable_name*.*attribute*}} **Section :** `{{#variable_name.attribute}}` `commands` `{{/variable_name.attribute}}` **Section inverse :** `{{^variable_name.attribute}}` `commands` `{{/variable_name.attribute}}`	Une interface nommée est définie sur la page Device (Périphérique) > Interfaces. Vous ne pouvez pas pointer vers des interfaces sans nom. Il existe une grande variété d'attributs disponibles dans le modèle d'interface. En outre, le modèle d'interface comprend des sous-objets, par exemple pour les adresses IP. Voici quelques-uns des principaux attributs que vous pourriez trouver utiles : • *variable_name*.**name** renvoie le nom logique de l'interface. • *variable_name*.**hardwareName** renvoie le nom du port de l'interface, tel que GigabitEthernet1/8. • *variable_name*.**managementOnly** est une valeur booléenne. TRUE (Vrai) signifie que l'interface est définie comme une interface de gestion uniquement. FALSE (Faux) signifie que l'interface est destinée au trafic traversant le périphérique. Vous pouvez utiliser cette option comme clé de section. • *variable_name*.**ipv4.ipAddress.ipAddress** renvoie l'adresse IPv4 de l'interface. • *variable_name*.**ipv4.ipAddress.netmask** renvoie le masque de sous-réseau pour l'adresse IPv4 de l'interface.
IP (variable simple)	**Variable :** {{*variable_name*}}	Une adresse IP IPv4 ou IPv6 unique, sans masque réseau ni longueur de préfixe.
Réseau (variable d'objet : le modèle API est NetworkObject)	**Variable (Network Objects (Objets réseau)) :** {{*variable_name*.*attribute*}} **Section (Group Objects (Groupe d'objets)) :** `{{#variable_name.networkObjects}}` `commands referring to one of` `  {{value}}` `  {{name}}` `{{/variable_name.networkObjects}}`	Un objet réseau ou un groupe défini sur la page Objects (Objets). Vous pouvez utiliser des sections pour traiter des groupes réseau. Voici les principaux attributs que vous pourriez trouver utiles : • {{*variable_name*.**name**}} renvoie le nom de l'objet ou du groupe réseau. • {{*variable_name*.**value**}} renvoie le contenu de l'adresse IP d'un objet réseau (mais pas d'un groupe réseau). Veillez à utiliser un objet réseau qui a le type de contenu approprié pour une commande donnée, par exemple une adresse d'hôte plutôt qu'une adresse de sous-réseau. • {{*variable_name*.**groups**}} renvoie la liste des objets réseau contenus dans un groupe réseau. Utilisez-le uniquement avec les variables qui pointent vers des groupes de réseau et utilisez-le sur une balise de section pour traiter de manière itérative le contenu du groupe. Utilisez {{**value**}} ou {{**name**}} pour récupérer le contenu de chaque objet réseau à tour de rôle.

Type de variable	Modèles de référence	Description
Numérique (variable simple)	**Variable :** {{*variable_name*}}	Un nombre entier. N'incluez pas de virgules, de décimales, de signes (comme le signe négatif) ou la notation hexadécimale. Pour les nombres non entiers, utilisez une variable de chaîne.
Port (variable d'objet : le modèle API est PortObject, tcpports ou udpports)	**Variable :** {{*variable_name.attribute*}}	Un objet de port TCP ou UDP défini sur la page Objects (Objets). Il doit s'agir d'un objet de port et non d'un groupe de ports. Voici les principaux attributs que vous pourriez trouver utiles : • {{*variable_name*.**port**}} renvoie le numéro de port. Le protocole n'est pas inclus. • {{*variable_name*.**name**}} renvoie le nom de l'objet de port.
Secret (variable d'objet : le modèle API est Secret)	**Variable :** {{*variable_name*.**password**}} Ou : {{{*variable_name*.**password**}}}	Un objet de clé secrète défini pour FlexConfig. La seule référence que vous devez faire est à l'attribut **password**, qui renvoie la chaîne chiffrée. Si le mot de passe comprend des caractères spéciaux tels que &, utilisez des accolades triples.
Chaîne (variable simple)	**Variable :** {{*variable_name*}}	Une chaîne de texte. Par exemple, les noms d'hôte, les noms d'utilisateur, etc.

Sections {{#key}} {{/key}} et sections inverses {{^key}} {{/key}}

Une section ou une section inverse est un bloc de commandes entre les balises de début et de fin de section, qui utilisent une clé comme critère de traitement. La façon dont la section est traitée dépend de s'il s'agit d'une section normale ou inverse :

- Une section normale (ou simplement une section) est traitée si la clé est TRUE (vrai) ou a un contenu non vide. Si la clé est FALSE (faux) ou si l'objet n'a pas de contenu, les commandes de la section ne sont pas configurées. La section est contournée.

  Voici la syntaxe d'une section normale.

```
{{#key}}
one or more commands
{{/key}}
```

- Une section inverse est l'opposé d'une section. Elle est traitée si la clé est FALSE (faux) ou si l'objet n'a pas de contenu. Si la clé est TRUE (vrai) ou si l'objet a du contenu, la section inverse est contournée.

  Voici la syntaxe d'une section inverse. La seule différence est qu'un signe d'attention remplace la balise de hachage.

```
{{^key}}
one or more commands
{{/key}}
```

Les rubriques suivantes expliquent les principales utilisations des sections et des sections inverses.

Comment traiter les variables à valeurs multiples

Le principal exemple de traitement d'une variable à valeurs multiples est une variable réseau qui pointe vers un groupe de réseaux. Comme le groupe contient plusieurs objets (sous l'attribut **objects**), vous pouvez parcourir de manière itérative les valeurs du groupe de réseau pour configurer la même commande plusieurs fois avec des valeurs différentes.

Bien qu'un groupe d'objets définisse les objets réseau contenus dans l'attribut des objets, ces objets n'incluent pas le contenu des objets contenus. Au lieu de cela, vous utilisez l'attribut **networkObjects** pour obtenir le contenu des objets contenus.

Par exemple, si vous avez un groupe de réseau nommé net-group avec les hôtes 192.168.10.0, 192.168.20.0 et 192.168.30.0, vous pouvez utiliser la technique suivante pour configurer une commande réseau pour chaque adresse pour le routage RIP. Notez que vous utilisez l'attribut **value** de l'objet réseau, car l'utilisation de **net-group.networkObjects** dans le début de la section implique que l'attribut de valeur sera extrait uniquement des objets membres. (Vous ne créez pas de variable distincte pour l'attribut « value » dans l'objet FlexConfig.)

```
router rip
{{#net-group.networkObjects}}
 network {{value}}
{{/net-group.networkObjects}}
```

Le système traduit la structure de section comme suit :

```
router rip
   network 192.168.10.0
   network 192.168.20.0
   network 192.168.30.0
```

Effectuer un traitement facultatif en fonction d'une valeur booléenne ou d'un objet vide



Remarque Les exemples de cette rubrique sont fournis uniquement à des fins d'illustration. Par exemple, vous ne pouvez pas utiliser FlexConfig pour configurer SNMP à partir de la version 6.7 ; vous devez plutôt utiliser la ressource SNMP de l'API Firewall Threat Defense.

Si le contenu de la variable dans la balise de début de section est TRUE (vrai), ou si un objet n'est pas vide, la section est traitée. Si une valeur booléenne est FALSE (faux) ou vide (comme un objet vide), la section est ignorée.

L'utilisation principale ici concerne les valeurs booléennes. Par exemple, vous pouvez créer une variable booléenne et placer des commandes dans une section régie par cette variable. Ensuite, si vous devez activer ou désactiver une section des commandes dans l'objet FlexConfig, il vous suffit de modifier la valeur de la variable booléenne; vous n'avez pas besoin de supprimer ces lignes du code. Cela permet d'activer ou de désactiver facilement les fonctionnalités.

Par exemple, vous pourriez vouloir pouvoir désactiver les interruptions SNMP si vous utilisez FlexConfig pour activer SNMP. Vous pouvez créer une variable booléenne nommée enable-traps et la définir initialement à TRUE (vrai). Ensuite, si vous devez désactiver les interruptions, vous n'avez qu'à modifier la variable, la remplacer par FALSE (faux), enregistrer l'objet, puis redéployer la configuration. La séquence de commandes pourrait ressembler à ce qui suit :

```
snmp-server enable
snmp-server host inside 192.168.1.5
snmp-server community clearTextString
{{#enable-traps}}
snmp-server enable traps all
{{/enable-traps}}
```

Vous pouvez également effectuer ce type de traitement en fonction de valeurs booléennes à l'intérieur d'un objet. Par exemple, vous pouvez vérifier si une interface est réservée à la gestion avant de configurer une caractéristique sur celle-ci. Dans l'exemple suivant, int-inside est une variable d'interface qui pointe vers l'interface nommée inside. FlexConfig configure les options d'interface liées à EIGRP sur l'interface uniquement si celle-ci n'est pas définie comme interface de gestion uniquement. Vous utiliserez une section inverse afin que les commandes ne soient configurées que si la valeur booléenne est FALSE (faux).

```
router eigrp 2
 network 192.168.1.0 255.255.255.0
{{^int-inside.managementOnly}}
interface {{int-inside.hardwareName}}
 hello interval eigrp 2 60
 delay 200
{{/int-inside.managementOnly}}
```

Référence aux objets Smart CLI dans un objet FlexConfig

Lorsque vous créez un objet FlexConfig, vous pouvez utiliser des variables pour pointer vers des objets que vous pouvez configurer dans le Gestionnaire de périphériques de pare-feu. Par exemple, vous pouvez créer des variables qui pointent vers des éléments d'interface ou des objets réseau.

Cependant, vous ne pouvez pas pointer vers des objets Smart CLI de la même manière.

Au lieu de cela, si vous créez un objet Smart CLI que vous devez utiliser dans une politique FlexConfig, vous saisissez simplement le nom de l'objet Smart CLI à l'emplacement approprié.

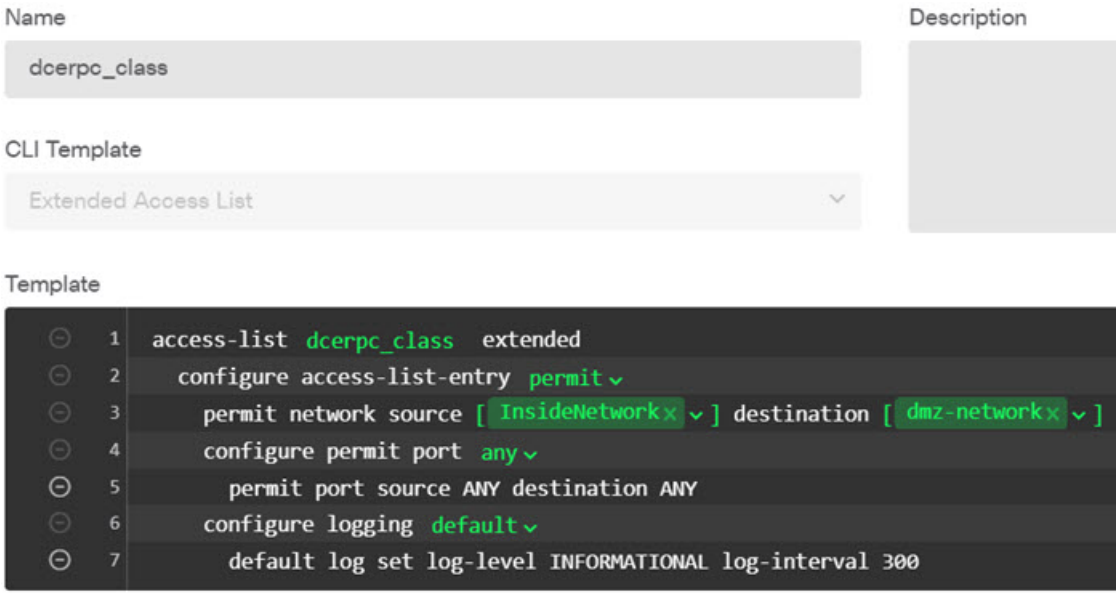
Par exemple, vous pouvez utiliser une liste d'accès étendue comme classe de trafic lorsque vous configurez l'inspection de protocole. Comme il existe un objet Smart CLI pour les listes d'accès étendues, vous devez utiliser l'objet Smart CLI pour créer l'ACL : vous ne pouvez pas utiliser la commande **access-list** dans l'objet FlexConfig.

Par exemple, si vous souhaitez activer l'inspection DCERPC entre les réseaux 192.168.1.0/24 et 192.168.2.0/24 globalement, vous procéderez comme suit.

Procédure

Étape 1 Créez des objets réseau distincts pour les deux réseaux. Par exemple, InsideNetwork et dmz-network.

Étape 2 Utilisez ces objets dans un objet de liste d'accès étendu Smart CLI.



Étape 3 Créez un objet FlexConfig qui pointe vers l'objet Smart CLI par son nom.

Par exemple, si l'objet est nommé « dcerpc_class », votre objet FlexConfig peut ressembler à ce qui suit. Notez que dans le modèle d'annulation, vous n'annulez pas la liste d'accès créée par l'objet Smart CLI, car cet objet n'est pas réellement créé par FlexConfig.



Étape 4 Ajoutez l'objet à la politique FlexConfig.

Configuration des objets de clé secrète

Le but d'un objet de clé secrète est de masquer les mots de passe ou les chaînes sensibles. Si vous ne voulez pas risquer que quelqu'un voie une chaîne utilisée dans un objet FlexConfig ou un modèle Smart CLI, créez un objet de clé secrète pour cette chaîne.

Procédure

Étape 1 Sélectionnez **Objects** (objets), puis **Clés secrètes** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Saisissez le mot de passe ou une autre chaîne secrète dans les champs **Password** (Mot de passe) et **Confirm Password** (Confirmer le mot de passe).

Le système masque le texte pendant que vous tapez.

Étape 5 Cliquez sur **OK**.

Prochaine étape

- S'il s'agit d'un nouvel objet, pour l'utiliser dans FlexConfig, modifiez un objet FlexConfig, créez une variable du type de clé secrète et sélectionnez l'objet. Ensuite, faites référence à la variable dans le corps de l'objet. Pour en savoir plus, consultez Création de variables dans un objet FlexConfig, à la page 885.
- Si vous modifiez un objet existant qui est utilisé dans un objet FlexConfig qui fait partie de la politique FlexConfig, vous devez déployer la configuration pour mettre à jour le périphérique avec la nouvelle chaîne.
- Dans les modèles Smart CLI, si une commande nécessite une clé secrète, vous verrez une liste de ces objets lors de la modification de la propriété concernée. Sélectionnez la clé appropriée selon l'usage prévu.

Dépannage de la politique FlexConfig

Après avoir modifié la politique FlexConfig, examinez attentivement les résultats du prochain déploiement. Si vous recevez un message « Le dernier déploiement a échoué » dans la boîte de dialogue Pending Changes (Modifications en attente), cliquez sur le lien **See Details** (Voir les détails). Le lien vous mène vers le journal d'audit, où vous pouvez trouver la tâche de déploiement qui a échoué. Ouvrez la tâche pour trouver les messages d'erreur spécifiques.

Si le déploiement échoue en raison d'un problème FlexConfig, les détails indiqueront l'objet FlexConfig contenant la commande incorrecte et afficheront la commande qui a échoué. Utilisez ces renseignements pour corriger l'objet et réessayer le déploiement. Le nom de l'objet est un lien. Cliquez dessus pour ouvrir la boîte de dialogue Edit (Modifier) de l'objet.

Par exemple, vous pourriez vouloir configurer la taille maximale de segment TCP (TCP MSS). Vous pouvez contrôler ce paramètre avec la commande **sysopt connection tcpmss**. Lorsqu'elle est configurée par

Gestionnaire de périphériques de pare-feu, la valeur par défaut Firewall Threat Defense pour cette option est 0, par rapport à la valeur ASA par défaut de 1380.

La valeur par défaut de l'ASA est conçue pour un traitement optimal lors de l'exécution d'un VPN IPv4 sur des interfaces qui utilisent la MTU par défaut de 1 500. Le système a besoin de 120 octets pour les en-têtes VPN. Pour IPv6, le système a besoin de 140 octets. La Firewall Threat Defense par défaut de 0 permet simplement aux points terminaux de négocier le MSS, qui est le paramètre idéal pour le trafic normal, surtout si vous utilisez différentes MTU sur les interfaces du périphérique, y compris des MTU supérieures à 1 500. Étant donné que le MSS TCP est un paramètre global et non propre à une interface, vous ne le modifieriez que si un pourcentage important de votre trafic passe par le VPN et que vous constatez une fragmentation excessive. Dans ce cas, vous pouvez définir le MSS TCP à MTU moins 120 (pour IPv4) ou 140 (pour IPv6), et utiliser la même MTU pour toutes les interfaces.

À titre d'illustration, supposons que vous souhaitiez définir le MSS TCP à 3 octets. La commande prend 48 octets comme valeur minimale, vous obtiendrez donc une erreur de déploiement semblable à ce qui suit :



L'erreur se compose des éléments suivants :

1. Le message d'erreur de déploiement, qui comprend le nom de l'objet FlexConfig qui a causé l'erreur. Le nom de l'objet est lié à la boîte de dialogue Edit (Modifier) afin que vous puissiez ouvrir rapidement l'objet et corriger l'erreur. Il s'agit de la première phrase du message.
2. Le texte commençant par « ERROR : » est le message renvoyé par le périphérique. C'est exactement ainsi qu'un ASA répondrait si vous saisissiez la commande erronée, sans le formatage d'un client SSH. Dans cet exemple, le message d'erreur est « ERROR : [3] est inférieur au MSS minimal autorisé de 48 par la RFC 791 ». Le texte qui commence par « Config Error » mentionne la ligne précise qui a généré le message d'erreur.
3. Le texte en noir correspond à la ligne réelle de l'objet FlexConfig qui a causé l'erreur. Vous devez corriger cette ligne. Dans cet exemple, si vous essayez d'adapter le trafic VPN IPv4 sur des interfaces MTU 1500 (cas courant), vous remplaceriez 3 par 1 380.

   Pour corriger cet exemple, vous pouvez laisser la console d'interface de ligne de commande ouverte et utiliser **show running-config all sysopt** pour voir tous les paramètres de commande **sysopt**. La plupart des commandes **sysopt** possèdent des valeurs par défaut adaptées à la plupart des usages, de sorte qu'elles n'apparaissent pas dans la configuration active. Le mot-clé **all** inclut ces paramètres par défaut dans la sortie.

Exemples de FlexConfig

Les rubriques suivantes fournissent quelques exemples d'utilisation de FlexConfig pour configurer les fonctionnalités.

Comment activer et désactiver les inspections globales par défaut

Certains protocoles intègrent des informations d'adressage IP dans le paquet de données de l'utilisateur ou ouvrent des canaux secondaires sur les ports affectés dynamiquement. Ces protocoles nécessitent que le système effectue une inspection approfondie des paquets afin que la NAT puisse être appliquée et que les canaux secondaires puissent être autorisés. Plusieurs moteurs d'inspection courants sont activés sur le système par défaut, mais vous devrez peut-être en activer d'autres ou désactiver les inspections par défaut, en fonction de votre réseau.

Pour voir la liste des inspections actuellement activées, utilisez la commande **show running-config policy-map**, soit dans la console CLI, soit dans une session SSH. Voici ce que vous verriez sur un système où aucune modification n'a été apportée à la configuration d'inspection. Dans cette sortie, la liste des commandes **inspect** à la fin de la sortie indique les inspections de protocole activées. Les commandes précédentes activent ces inspections sur la classe de trafic inspection_default (qui contient les protocoles normaux et, le cas échéant, les numéros de port pour le protocole inspecté). Cette classe fait partie de la carte de politiques global_policy, qui applique ces inspections à toutes les interfaces à l'aide d'une commande service-policy qui ne s'affiche pas dans la sortie. Par exemple, l'inspection ICMP est effectuée sur tout le trafic ICMP qui passe par le périphérique.

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
!
```

Remarque Pour une description détaillée de chaque inspection, consultez le *Guide de configuration des pare-feu Cisco ASA* disponible sur le site https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html.

La procédure suivante vous montre comment activer ou désactiver les inspections dans cette classe d'inspection par défaut appliquée globalement. À des fins d'illustration, l'exemple :

- Active le PPTP (Protocole Point-to-Point Tunneling). Ce protocole est utilisé pour tunnelliser une connexion point à point entre deux points terminaux.
- Désactive le SIP (Session Initiation Protocol). Vous ne devez généralement désactiver le protocole SIP que si l'inspection cause des problèmes dans le réseau. Toutefois, si vous désactivez le protocole SIP, vous devez vous assurer que vos stratégies de contrôle d'accès autorisent le trafic SIP (UDP/TCP 5060) et tous les ports alloués dynamiquement, et que vous n'avez pas besoin de prise en charge de la NAT pour les connexions SIP. Ajustez les politiques de contrôle d'accès et de NAT en conséquence à l'aide des pages standard, et non par l'intermédiaire de FlexConfig.

Avant de commencer

Une bonne planification vous aidera à utiliser FlexConfig efficacement. Dans cet exemple, nous modifions deux inspections différentes et non liées, bien que nous apportions les modifications dans la même classe de trafic. Mais il est fort possible que si vous devez modifier ces politiques, vous le fassiez de manière indépendante.

Par conséquent, nous vous recommandons de créer des objets FlexConfig distincts pour chaque inspection dans cet exemple. De cette façon, vous pouvez facilement modifier vos paramètres pour une inspection sans modifier l'autre et sans avoir à modifier l'objet FlexConfig.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Créez l'objet pour activer l'inspection PPTP.

a) Cliquez sur le bouton + pour créer un nouvel objet.

b) Saisissez un nom pour l'objet. Par exemple, **Enable_PPTP_Global_Inspection**.

c) Dans l'éditeur **Template** (Modèle), saisissez les lignes suivantes, y compris les indentations.

```
policy-map global_policy
 class inspection_default
  inspect pptp
```

d) Dans l'éditeur **Negate Template** (Modèle d'annulation), saisissez les lignes nécessaires pour annuler cette configuration.

Tout comme vous devez inclure les commandes parentes pour entrer dans le sous-mode approprié pour une commande afin de l'activer, vous devez également inclure ces commandes dans le modèle de négation.

Le modèle d'annulation sera appliqué si vous supprimez cet objet de la politique FlexConfig (après l'avoir déployé avec succès), et également lors d'un déploiement infructueux (pour réinitialiser la configuration à son état précédent).

Ainsi, pour cet exemple, le modèle de négation serait le suivant :

```
policy-map global_policy
 class inspection_default
```

```
no inspect pptp
```

L'objet doit ressembler à ce qui suit :



Remarque
Comme la classe inspection_default comporte d'autres commandes d'inspection activées, vous ne souhaitez pas annuler la classe entière. De même, la carte de politiques global_policy comprend ces autres inspections, et vous ne souhaitez pas non plus annuler la carte de politiques.

e) Cliquez sur **OK** pour enregistrer l'objet.

Étape 4 Créez l'objet pour désactiver l'inspection SIP.

a) Cliquez sur le bouton **+** pour créer un nouvel objet.
b) Saisissez un nom pour l'objet. Par exemple, **Disable_SIP_Global_Inspection**.
c) Dans l'éditeur **Template** (Modèle), saisissez les lignes suivantes, y compris les indentations.

```
policy-map global_policy
 class inspection_default
  no inspect sip
```

d) Dans l'éditeur **Negate Template** (Modèle d'annulation), saisissez les lignes nécessaires pour annuler cette configuration.

La commande « negate » pour une commande « no » de désactivation est la commande qui active la fonctionnalité. Ainsi, le modèle « annuler » ne comprend pas seulement les commandes pour désactiver

une fonctionnalité, il s'agit des commandes pour inverser ce que vous faites dans le modèle « positif ». L'objectif du modèle d'annulation est d'annuler vos modifications.

Ainsi, pour cet exemple, le modèle de négation serait le suivant :

```
policy-map global_policy
 class inspection_default
  inspect sip
```

L'objet doit ressembler à ce qui suit :



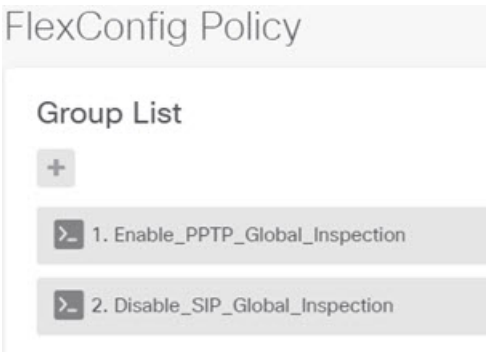
e) Cliquez sur **OK** pour enregistrer l'objet.

Étape 5 Ajoutez les objets à la politique FlexConfig.

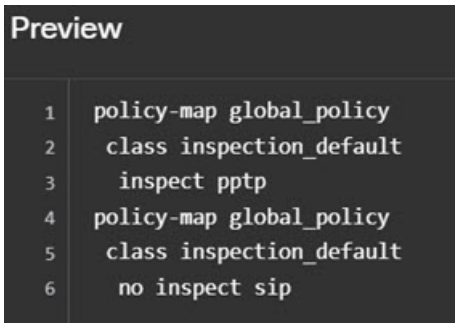
La création d'un objet n'est pas suffisante. Les objets sont déployés uniquement si vous les ajoutez à la politique FlexConfig (et enregistrez vos modifications). Cela vous permet de tester des objets (et de les laisser partiellement terminés) sans risquer d'échecs de déploiement sur un travail inachevé. Vous pouvez ensuite activer ou désactiver facilement des fonctionnalités en ajoutant et en supprimant des objets : il n'est pas nécessaire de recréer l'objet à chaque fois.

a) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières.
b) Cliquez sur + dans la liste des groupes.
c) Sélectionnez les objets Enable_PPTP_Global_Inspection et Disable_SIP_Global_Inspection, puis cliquez sur **OK**.

La liste des groupes doit ressembler à ce qui suit :



L'aperçu doit être mis à jour avec les commandes du modèle. Vérifiez que vous voyez les commandes attendues.



d) Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant déployer la politique.

Étape 6 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Étape 7 Dans la console d'interface de ligne de commande ou une session SSH, utilisez la commande **show running-config policy-map** et vérifiez que la configuration en cours d'exécution comporte les modifications correctes.

Dans la sortie suivante, notez que **inspect pptp** est ajouté au bas de la classe inspection_default et que **inspect sip** ne figure plus dans la classe. Cela confirme que les modifications définies dans l'objet FlexConfig ont été déployées avec succès.

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
```

```
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
!
```

Comment annuler vos modifications FlexConfig

Si vous saisissez un modèle de négation correct dans un objet FlexConfig, la suppression des modifications apportées à l'aide de cet objet est simple. Vous supprimez simplement l'objet de la politique FlexConfig et lors du prochain déploiement, le système utilise votre modèle de négation pour annuler vos modifications.

Vous n'avez pas besoin de créer un nouvel objet pour annuler vos modifications.

L'exemple suivant montre comment réactiver l'inspection SIP globale. L'exemple rétablit la modification expliquée dans Comment activer et désactiver les inspections globales par défaut, à la page 895, qui a désactivé l'inspection SIP.

Avant de commencer

Vérifiez que l'objet FlexConfig dispose du bon modèle de négation. Si ce n'est pas le cas, modifiez l'objet pour corriger le modèle de négation.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Policy (Politique FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Cliquez sur le **X** à droite de l'entrée de l'objet **Disable_SIP_Global_Inspection** dans la politique FlexConfig pour le supprimer de la politique.



Les commandes de l'objet sont supprimées de l'aperçu. Les commandes d'annulation ne sont pas ajoutées à l'aperçu, elles seront exécutées en arrière-plan.

Étape 4 Cliquez sur **Save** (enregistrer).

Étape 5 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Étape 6 Dans la console d'interface de ligne de commande ou une session SSH, utilisez la commande **show running-config policy-map** et vérifiez que la configuration en cours d'exécution comporte les modifications correctes.

Dans le résultat suivant, notez que **inspect sip** est ajouté au bas de la classe inspection_default. Cela confirme que les modifications définies dans l'objet FlexConfig ont été déployées avec succès. (L'ordre n'est pas important dans cette classe, donc peu importe que **inspect sip** se trouve à la fin et non à son emplacement d'origine.)

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
  inspect sip
!
```

Comment activer les inspections pour les classes de trafic uniques

Dans cet exemple, nous activerons l'inspection PPTP pour le trafic entre deux points terminaux sur une interface spécifique. Cela cible l'inspection uniquement sur les points terminaux qui ont un tunnel point à point configuré entre eux.

L'interface de ligne de commande requise pour activer l'inspection PPTP entre 2 points terminaux implique les éléments suivants :

1. Une liste de contrôle d'accès avec la source et la destination définies pour les adresses IP des hôtes du terminal.
2. Une classe de trafic qui fait référence à cette liste de contrôle d'accès.
3. Une carte de politiques qui comprend la classe de trafic et qui active l'inspection PPTP sur la classe de trafic.
4. Une politique de service qui applique la carte de politiques à l'interface souhaitée. Il s'agit de l'étape qui active la politique et permet l'inspection.

Remarque Pour obtenir une description détaillée des politiques de service liées aux inspections, consultez le *guide de configuration de pare-feu Cisco ASA* disponible sur le site https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

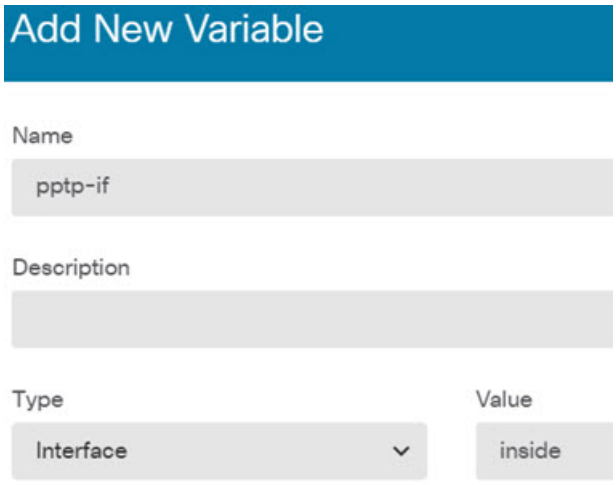
Étape 3 Cliquez sur le bouton + pour créer un nouvel objet.

Étape 4 Saisissez un nom pour l'objet. Par exemple, **Enable_PPTP_Inspection_on_Interface**.

Étape 5 Ajoutez une variable pour l'interface interne.

a) Cliquez sur le signe + au-dessus de la liste des variables.
b) Saisissez un nom pour la variable, par exemple, **pptp-if**.
c) Pour **Type**, sélectionnez **Interface**.
d) Pour **Value** (Valeur), sélectionnez l'interface **inside**.

La boîte de dialogue doit ressembler à ce qui suit :



e) Cliquez sur **Add** (ajouter).

Étape 6 Dans l'éditeur **Template** (Modèle), saisissez les lignes suivantes, y compris les indentations.

```
access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
class-map MATCH_CMAP
 match access-list MATCH_ACL
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
service-policy PPTP_POLICY interface {{pptp-if.name}}
```

Notez que pour utiliser la variable, vous devez saisir le nom de la variable entre double crochets. Vous devez également utiliser la notation par point pour choisir l'attribut que vous souhaitez récupérer, car l'objet qui définit une interface comporte de nombreux attributs. Comme le nom de l'interface est contenu dans l'attribut « name », la saisie de **{{pptp-if.name}}** récupère la valeur de l'attribut de nom de l'interface attribuée à la variable. Si vous devez modifier l'interface pour l'inspection PPTP, il vous suffit de sélectionner une interface différente dans la définition de la variable.

Étape 7 Dans l'éditeur **Negate Template** (Modèle d'annulation), saisissez les lignes nécessaires pour annuler cette configuration.

Pour cet exemple, nous supposerons que la carte de classes, la carte de politiques et la politique de service existent dans le seul but d'appliquer l'inspection PPTP. Ainsi, dans le modèle d'annulation, nous souhaitons supprimer tous ces éléments.

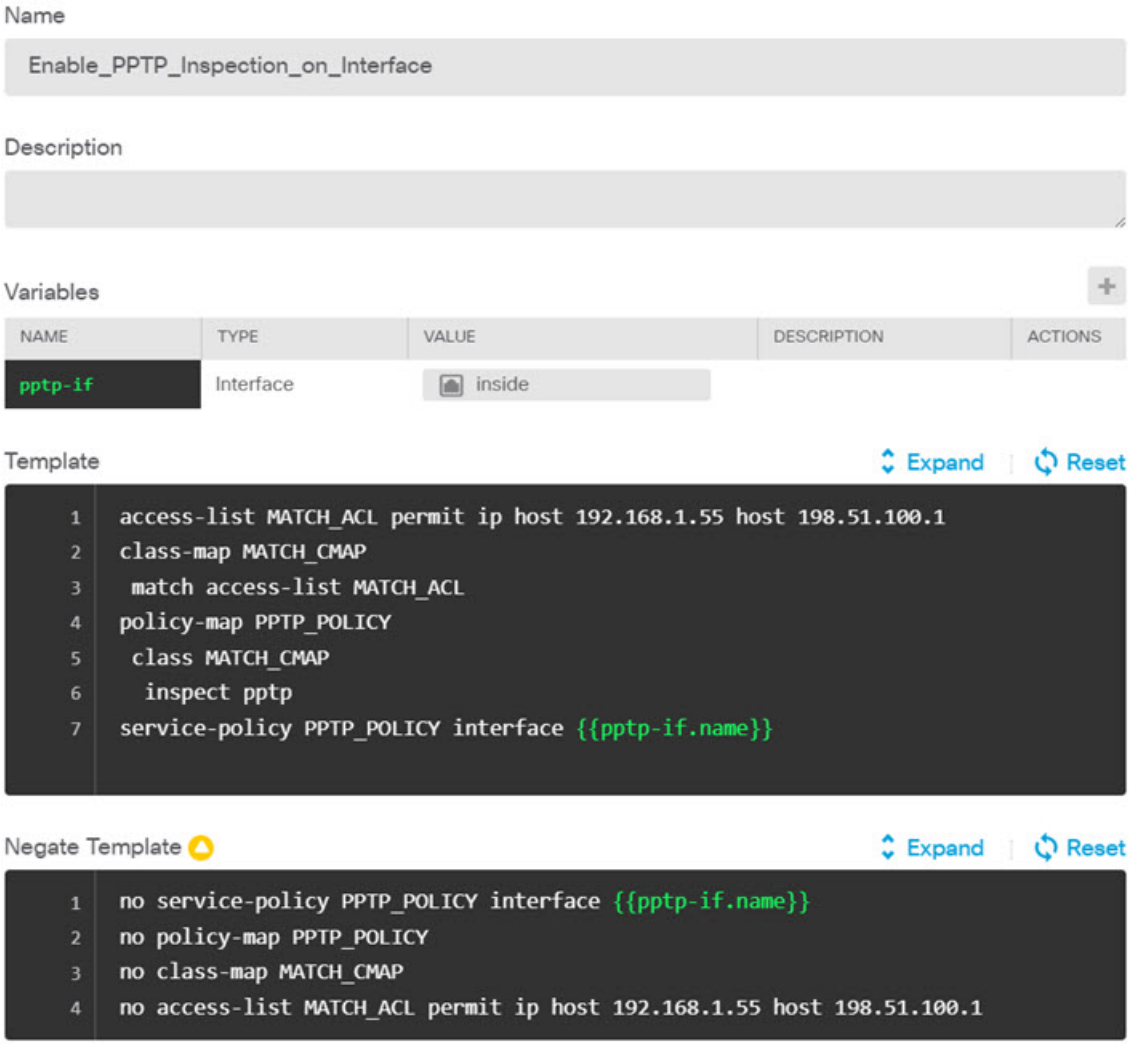
Si, toutefois, vous ajoutez actuellement l'inspection PPTP à une politique de service existante sur une interface, vous n'annulerez pas la carte de politiques ou la politique de service. Vous pouvez soit annuler la classe de la carte des politiques, soit désactiver simplement l'inspection au sein de la classe au sein de la carte des politiques. Vous devez avoir une compréhension claire de ce que vous mettez en œuvre dans les autres objets FlexConfig pour vous assurer que votre modèle d'annulation n'a pas de conséquences inattendues.

Lors de la suppression d'éléments imbriqués, vous devez le faire dans l'ordre inverse dans lequel vous les avez créés. Ainsi, vous commencez par supprimer la politique de service et terminez par la suppression de la liste d'accès. Sinon, vous tenteriez de supprimer des objets qui sont en cours d'utilisation, et le système renvoyera des erreurs et ne vous permettra pas de le faire.

```
no service-policy PPTP_POLICY interface {{pptp-if.name}}
```

```
no policy-map PPTP_POLICY
no class-map MATCH_CMAP
no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 8 Cliquez sur **OK** pour enregistrer l'objet.

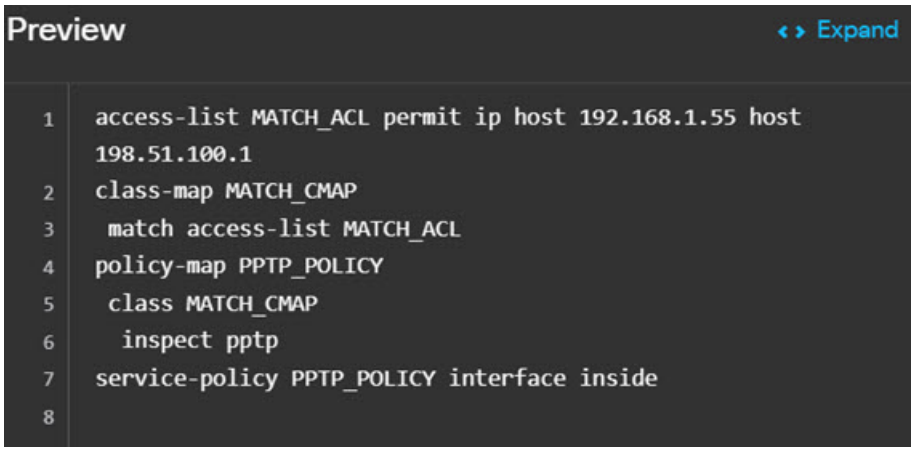
Étape 9 Ajoutez les objets à la politique FlexConfig.

a) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières.
b) Cliquez sur + dans la liste des groupes.
c) Sélectionnez l'objet **Enable_PPTP_Inspection_on_Interface** et cliquez sur **OK**.

La liste des groupes doit ressembler à ce qui suit :



L'aperçu doit être mis à jour avec les commandes du modèle. Vérifiez que vous voyez les commandes attendues, comme le montre le graphique suivant. Remarquez que la variable d'interface se résout en nom « inside » dans l'aperçu. Portez une attention particulière aux variables : si elles ne se résolvent pas correctement dans l'aperçu, elles ne seront pas déployées correctement. Modifiez l'objet FlexConfig jusqu'à ce que vous obteniez la traduction de variable correcte dans l'aperçu.



d) Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant déployer la politique.

Étape 10 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.



b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Étape 11 Dans la console d'interface de ligne de commande ou une session SSH, utilisez des variantes de la commande **show running-config** et vérifiez que la configuration en cours d'exécution comporte les modifications correctes.

Vous pouvez saisir **show running-config** et examiner l'ensemble de la configuration CLI, ou utiliser les commandes suivantes pour vérifier chaque partie de cette configuration :

- **show running-config access-list MATCH_ACL** pour vérifier l'ACL.

- **show running-config class** pour vérifier la carte de classe. Cette commande affichera toutes les cartes de classe.
- **show running-config policy-map PPTP_POLICY** pour vérifier la configuration des classes et de la carte de politiques.
- **show running-config service-policy** pour vérifier que la carte des politiques a été appliquée à l'interface. Cela affichera toutes les politiques de service.

Le résultat suivant montre cette séquence de commandes, et vous pouvez voir que la configuration est correctement appliquée.

```
> show running-config access-list MATCH_ACL
access-list MATCH_ACL extended permit ip host 192.168.1.55 host 198.51.100.1

> show running-config class
!
class-map MATCH_CMAP
 match access-list MATCH_ACL
class-map inspection_default
 match default-inspection-traffic
!

> show running-config policy-map PPTP_POLICY
!
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
!
> show running-config service-policy
service-policy global_policy global
service-policy PPTP_POLICY interface inside
```

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.

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.